POLITYKA OCHRONY DANYCH OSOBOWYCH

Niniejszy dokument zatytułowany „Polityka ochrony danych osobowych" (dalej jako: Polityka) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w placówce, której Administratorem danych osobowych jest – LUCARE CONCEPT Spółka z ograniczoną odpowiedzialnością z siedzibą w Gliwicach, ul. Kolibrów 38, 44-122 Gliwice, NIP: 6312741790, KRS: 0001246893, w ramach której prowadzi podmiot leczniczy: LUCARE - MED & AESTHETIC CONCEPT, wpisany do Rejestru Podmiotów Wykonujących Działalność Leczniczą pod numerem 54497412300012, (dalej jako: Gabinet).

Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu Rozporządzenia 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 (ogólne rozporządzenie o ochronie danych) Dz.U.UE.L.2018.127.2 t. j.(dalej jako RODO).

§1 Postanowienia ogólne

1. Administratorem danych osobowych jest [Administrator]. Polityka ma zastosowanie do wszystkich osób przetwarzających dane z upoważnienia Administratora, niezależnie od podstawy zatrudnienia lub współpracy.
2. Dane osobowe są przetwarzane zgodnie z RODO, ustawą o ochronie danych osobowych, przepisami dotyczącymi praw pacjenta i dokumentacji medycznej, działalności leczniczej, systemu informacji w ochronie zdrowia oraz innymi przepisami mającymi zastosowanie do działalności placówki.
3. Placówka stosuje zasady: zgodności z prawem, rzetelności i przejrzystości; ograniczenia celu; minimalizacji danych; prawidłowości; ograniczenia przechowywania; integralności i poufności oraz rozliczalności.
4. Dane dotyczące zdrowia i inne szczególne kategorie danych podlegają podwyższonej ochronie.

§ 2. System ochrony danych i odpowiedzialność

1. Administrator odpowiada za wdrożenie, utrzymanie i okresowy przegląd systemu ochrony danych.
2. Administrator ustala role i odpowiedzialności, nadaje i cofa upoważnienia oraz zapewnia, aby osoby mające dostęp do danych przetwarzały je wyłącznie w zakresie niezbędnym do wykonywania obowiązków.
3. Jeżeli wyznaczono Inspektora Ochrony Danych, jego dane kontaktowe i zadania określa się w odrębnej dokumentacji.
4. Personel jest zobowiązany do zachowania poufności danych, w tym po ustaniu zatrudnienia lub współpracy.

§ 3. Inwentaryzacja i Rejestr Czynności Przetwarzania

1. Placówka identyfikuje procesy, systemy, zbiory danych, kategorie osób, cele i podstawy prawne przetwarzania oraz odbiorców danych.
2. Prowadzony jest Rejestr Czynności Przetwarzania obejmujący co najmniej: cele, kategorie osób i danych, odbiorców, planowane terminy usunięcia oraz ogólny opis zabezpieczeń.
3. Rejestr obejmuje w szczególności: udzielanie świadczeń zdrowotnych i dokumentację medyczną, rejestrację i kontakt z pacjentem, EDM, rozliczenia, kadry i płace, rekrutację, kontrahentów, obsługę korespondencji, systemy IT, monitoring oraz marketing lub publikację wizerunku, jeżeli takie procesy występują.
4. Rejestr jest aktualizowany przy zmianach procesów, systemów, dostawców, podstaw prawnych lub zakresu danych.

§ 4. Podstawy i cele przetwarzania

1. Każdy proces musi mieć określony, zgodny z prawem cel i właściwą podstawę przetwarzania.
2. Dane pacjentów niezbędne do udzielania świadczeń, prowadzenia i przechowywania dokumentacji medycznej są przetwarzane w zakresie wynikającym z obowiązków prawnych placówki oraz przesłanek dotyczących świadczenia opieki zdrowotnej.
3. Zgoda nie jest stosowana jako zastępcza podstawa tam, gdzie przetwarzanie jest konieczne z mocy prawa lub do świadczenia opieki zdrowotnej. Jeżeli zgoda jest właściwą podstawą, placówka dokumentuje jej udzielenie i umożliwia jej wycofanie.
4. Cele dodatkowe, takie jak marketing lub publikacja wizerunku, są wyraźnie oddzielane od procesu leczenia i mają odrębnie ustaloną podstawę prawną.

§ 5. Dokumentacja medyczna i EDM

1. Placówka prowadzi, przechowuje, zabezpiecza i udostępnia dokumentację medyczną zgodnie z właściwymi przepisami.
2. Dostęp do dokumentacji medycznej i EDM otrzymują wyłącznie osoby upoważnione, w zakresie wynikającym z ich zadań.
3. Systemy EDM powinny umożliwiać identyfikację użytkowników, zarządzanie rolami i uprawnieniami, rejestrowanie istotnych operacji oraz wykonywanie kopii zapasowych.
4. Nie usuwa się danych z dokumentacji medycznej wyłącznie na podstawie żądania pacjenta, jeżeli dalsze przechowywanie wynika z obowiązku prawnego. Żądania dotyczące danych rozpatruje się z uwzględnieniem przepisów szczególnych o dokumentacji medycznej.

6. Obowiązki informacyjne

1. Przy pozyskiwaniu danych placówka przekazuje wymagane informacje w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie.
2. Klauzule informacyjne dostosowuje się do poszczególnych grup, w szczególności pacjentów, personelu, kandydatów, kontrahentów, użytkowników strony internetowej i osób objętych monitoringiem.
3. Jeżeli dane pozyskiwane są z innego źródła niż od osoby, której dotyczą, realizuje się obowiązek informacyjny w zakresie i terminach przewidzianych prawem, chyba że zachodzi wyjątek ustawowy.
4. Zmiana celu przetwarzania wymaga oceny zgodności i przekazania osobie odpowiedniej informacji przed dalszym przetwarzaniem.

§ 7. Realizacja praw osób

1. Placówka zapewnia obsługę praw wynikających z RODO, w tym prawa dostępu, sprostowania, usunięcia, ograniczenia, sprzeciwu oraz przenoszenia danych w przypadkach przewidzianych prawem.
2. Przed realizacją żądania placówka może zweryfikować tożsamość w zakresie adekwatnym do ryzyka, szczególnie gdy żądanie dotyczy danych medycznych.
3. Odpowiedzi udziela się bez zbędnej zwłoki, co do zasady w terminie jednego miesiąca od otrzymania żądania. W przypadkach przewidzianych RODO termin może zostać przedłużony, o czym osoba jest informowana wraz z przyczynami.
4. Dostęp do danych na podstawie RODO oraz udostępnienie dokumentacji medycznej są traktowane jako odrębne uprawnienia i obsługiwane zgodnie z właściwymi przepisami.
5. Każde żądanie i sposób jego realizacji są dokumentowane.

§ 8. Minimalizacja i retencja

1. Placówka przetwarza tylko dane adekwatne i niezbędne do określonych celów.
2. Zakres formularzy, dostępów, raportów i eksportów danych podlega okresowym przeglądom.
3. Okresy przechowywania ustala się według obowiązków prawnych, celu przetwarzania i okresów przedawnienia roszczeń. Dla dokumentacji medycznej stosuje się okresy wynikające z przepisów szczególnych.
4. Po upływie właściwego okresu dane są bezpiecznie usuwane, anonimizowane albo niszczone, chyba że istnieje podstawa do dalszego przechowywania.
5. Zasady retencji obejmują również kopie zapasowe, archiwa, pocztę elektroniczną oraz dokumentację papierową.

§ 9. Upoważnienia i kontrola dostępu

1. Dostęp do danych nadawany jest zgodnie z zasadą minimalnych uprawnień i potrzebą wiedzy.

2. Placówka prowadzi ewidencję osób upoważnionych oraz dokumentuje nadanie, zmianę i cofnięcie dostępu.
3. Uprawnienia są niezwłocznie aktualizowane przy zmianie stanowiska, obowiązków lub zakończeniu współpracy.
4. Konta użytkowników są indywidualne. Zabrania się udostępniania haseł i korzystania z kont innych osób.
5. Dostęp administratorów systemów i serwisu zewnętrznego ogranicza się do zakresu niezbędnego do wykonania usługi i podlega odpowiednim zabezpieczeniom.

§ 10. Podmioty zewnętrzne i udostępnianie danych

1. Przed powierzeniem przetwarzania Administrator weryfikuje, czy dostawca daje wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, a relację reguluje odpowiednią umową.
2. Placówka prowadzi wykaz podmiotów przetwarzających i okresowo ocenia współpracę, w szczególności dostawców EDM, hostingu, IT, księgowości i usług archiwizacyjnych – jeżeli występują.
3. Każdorazowo ustala się właściwą rolę strony. Podmiot otrzymujący dane medyczne nie zawsze jest procesorem; w określonych sytuacjach może działać jako odrębny administrator, np. gdy realizuje własne obowiązki w zakresie świadczeń zdrowotnych.
4. Udostępnianie dokumentacji medycznej odbywa się wyłącznie osobom i podmiotom uprawnionym oraz po odpowiedniej weryfikacji podstawy i tożsamości.

§ 11. Bezpieczeństwo danych

1. Placówka wdraża środki techniczne i organizacyjne adekwatne do ryzyka, charakteru danych oraz skali przetwarzania.
2. Stosuje się w szczególności: kontrolę dostępu, silne uwierzytelnianie tam, gdzie jest zasadne, aktualizacje systemów, ochronę antymalware, kopie zapasowe, zabezpieczenie urządzeń i nośników, szyfrowanie w uzasadnionych przypadkach, bezpieczną transmisję, ochronę dokumentacji papierowej oraz zasady czystego biurka i ekranu.
3. Kopie zapasowe są wykonywane i okresowo testowane pod kątem możliwości odtworzenia.
4. Personel odbywa szkolenia i jest informowany o zagrożeniach, w tym phishingu, błędnym adresowaniu wiadomości, utracie urządzeń i nieuprawnionym ujawnieniu dokumentacji.
5. Placówka okresowo ocenia skuteczność zabezpieczeń i dokumentuje wyniki przeglądów.

§ 12. Naruszenia ochrony danych

1. Każdy pracownik i współpracownik niezwłocznie zgłasza Administratorowi podejrzenie utraty, zniszczenia, nieuprawnionego dostępu, ujawnienia lub innego naruszenia ochrony danych.
2. Placówka prowadzi rejestr naruszeń i dokumentuje okoliczności, skutki, ocenę ryzyka oraz podjęte działania.
3. Jeżeli naruszenie może powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator dokonuje zgłoszenia Prezesowi UODO bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 72 godzin od stwierdzenia naruszenia.
4. Jeżeli naruszenie może powodować wysokie ryzyko dla osoby, placówka zawiadamia ją bez zbędnej zwłoki, chyba że zachodzi przewidziany prawem wyjątek.
5. Po incydencie wdraża się działania naprawcze i zapobiegawcze.

§ 13. Ocena ryzyka, DPIA

1. Placówka okresowo ocenia ryzyko dla praw i wolności osób, w szczególności przy przetwarzaniu danych o zdrowiu, wdrażaniu nowych systemów, monitoringu, usługach chmurowych i nowych technologiach.
2. Jeżeli planowane przetwarzanie może powodować wysokie ryzyko, przed jego rozpoczęciem przeprowadza się ocenę skutków dla ochrony danych (DPIA), gdy wymagają tego przepisy.
3. Ochrona danych jest uwzględniana już na etapie projektowania procesów, wyboru systemów i dostawców oraz przy domyślnych ustawieniach usług.
4. Istotne zmiany technologiczne lub organizacyjne podlegają ponownej ocenie ryzyka.

§ 14. Transfer danych poza EOG

1. Przed przekazaniem danych poza Europejski Obszar Gospodarczy placówka identyfikuje odbiorcę, lokalizację przetwarzania i podstawę transferu.
2. Transfer może następować wyłącznie przy spełnieniu wymogów rozdziału V RODO, w tym zastosowaniu właściwego mechanizmu transferowego i – gdy jest to potrzebne – dodatkowych zabezpieczeń.
3. Dotyczy to również dostawców usług chmurowych, poczty, analityki, hostingu i innych narzędzi, jeżeli wiążą się z transferem danych.

§ 15. Monitoring wizyjny

1. Monitoring może być stosowany wyłącznie dla jasno określonego, zgodnego z prawem celu, po ocenie niezbędności, proporcjonalności i wpływu na prywatność.

2. Obszar monitorowany jest odpowiednio oznaczony, a osoby otrzymują wymagane informacje o przetwarzaniu.

_____

Za Administratora – Prezes Zarządu