POLITICA DE CONFIDENTIALITATE SI SECURITATE A PRELUCRARII DATELOR CU CARACTER PERSONAL A CLINICII DR. LEVENTER

Prezenta politica de securitate a fost creata avand in vedere:

- Faptul ca **DERMASTYLE S.R.L.** cu sediul in Bucuresti, Sos. Ghe. Ionescu Sisesti nr. 72D, sector 1, inregistrata la Registrul Comertului sub nr. J40/937/2002, cod unic de înregistrare RO 14444615, legal reprezentata prin D-na Mihaela Leventer, in calitate de administrator (denumita in continuare "**Clinica**" sau "**Noi**") desfasoara o activitate care presupune procesarea unor categorii de date cu caracter personal,

- intrarea in vigoare incepand cu data de 25 mai 2018 a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (denumit in continuare "**GDPR**"),

- obligatia impusa de GDPR de a asigura masuri de securitate tehnice si organizatorice adecvate tuturor activitatilor de procesare a datelor cu caracter personal;

- dedicarea noastra in vederea asigurarii celor mai inalte standarde de securitate, avand in vedere datele sensibile prelucrate si increderea pe care pacientii nostri ne-o acorda.

1. ANGAJAMENT

Clinica prelucreaza date cu caracter personal in scopuri legitime, cu respectarea tuturor principiilor impuse de GDPR si de practicile comerciale etice. Protejarea sigurantei si securitatii datelor personale este importanta pentru Clinica si aceasta politica descrie cadrul organizatoric implementat pentru asigurarea conformitatii prelucrarii.

Obiectivul principal al acestei Politici de Confidentialitate si Securitate este de a contribui la desfasurarea activitatii societatii cu respectarea prevederilor legale specifice si de a minimiza riscurile prin prevenirea incidentelor si, in cazul improbabil al unor astfel de incidente, reducerea impactului lor asupra persoanei vizate.

Ne propunem sa avem o relatie bazata pe incredere, transparenta, buna-credinta si etica in relatia cu toti partenerii, colaboratorii si angajatii nostri.

2. DEFINITII

"Date cu caracter personal" înseamnă orice informații privind o persoană fizică identificată sau identificabilă **(„persoana vizată")**; o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la

unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.

„Prelucrare” înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea.

„**Pseudonimizare**” înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile.

„**Operator**” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern.

„**Persoană împuternicită de operator**” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului.

„**Parte terță**” înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal.

„**Destinatar**” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării.

„**Consimțământ**” al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate.

„**Restricționarea prelucrării**” înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora.

3. PRINCIPIILE POLITICII DE SECURITATE

Clinica proceseaza datele cu caracter personal cu care vine in contact cu respectarea urmatoarelor principii:

- **Protejarea drepturilor si libertatilor fundamentale** ale persoanelor vizate;

- **Legalitate, echitate si transparenta** – datele cu caracter personal sunt prelucrate cu buna credinta si in conformitate cu dispozitiile legale in vigoare, intr-un mod echitabil si transparent fata de persoana vizata;

- **Scopuri determinate, explicite si legitime** – Prelucrarea datelor cu caracter personal de catre Clinica se face in scopuri determinate, explicite si legitime si nu sunt prelucrate ulterior intr-un mod incompatibil cu aceste scopuri;

- **Temei legal** – Clinica se va asigura ca orice procesare a datelor cu caracter personal va avea un temei bine determinat, precum prevederi legale, consimtamantul persoanei vizate, executarea contractelor, interesul legitim al Clinica (care nu va contraveni intereselor superioare ale persoanei vizate);

- **Limitare prin raportare la scop** – Clinica proceseaza datele cu caracter personal numai daca sunt adecvate, relevante si limitate la ceea ce este necesar in raport cu scopurile in care sunt prelucrate;

- **Limitare prin raportare la timp** – Clinica pastreaza datele persoanelor vizate pe o perioada care nu depaseste perioada necesara indeplinirii scopurilor in care sunt prelucrate datele;

- **Exactitate si acuratete** – Clinica proceseaza date cu caracter personal intr-un mod precis si ia masuri rezonabile pentru a se asigura ca datele inexacte de care ia cunostinta sunt sterse sau rectificate;

- **Securitate** – Clinica este dedicata asigurarii securitatii tuturor datelor cu caracter personal pe care le prelucreaza si face demersuri constante pentru a atinge acest scop, inclusiv prin instruirea angajatilor, colaboratorilor si partenerilor sai.

4. CATEGORII DE PERSOANE VIZATE

Clinica proceseaza date cu caracter personal ale urmatoarelor categorii de persoane vizate:

- Pacientii nostri, persoane fizice;
- Angajatii/colaboratorii proprii;
- Angajatii/colaboratorii partenerilor comerciali;
- Dupa caz, alte persoane fizice care interactioneaza cu societatea in cursul activitatii acesteia.

5. DATELE COLECTATE

In functie de specificul fiecarei relatii, Clinica poate procesa urmatoarele categorii de date cu privire la persoanele vizate:

- Nume si prenume;
- Date de contact: Telefon, adresa de e-mail;
- Date de identificare, conform cartii de identitate / pasaportului;
- Date de sanatate privind pacientii;
- Date privind studiile;
- Date profesionale: loc de munca, pozitie, vechime, experienta profesionala;
- Date furnizate direct prin e-mail sau prin alte modalitati de catre persoanele vizate;
- Date colectate despre angajati si familiile acestora, in scopul respectarii contractului de munca si a prevederilor legale in domeniul muncii;
- Date de localizare prin sisteme GPS;
- Imagine si voce.

Datele cu caracter personale mentionate mai sus au caracter exemplificativ.

Aceste date pot fi colectate din urmatoarele **surse**:

- De la clientii Clinicii in momentul in care doresc sa acceseze serviciile noastre;
- Din contracte si documente auxiliare acestora, inclusiv in executarea relatiilor de munca/colaborare;
- ca urmare a furnizarii acestora direct de catre persoana vizata – cu obtinerea consimtamantului in cazurile prevazute de lege; in unele cazuri, prin faptul ca persoana vizata ne transmite anumite informatii de buna voie catre noi prin orice canal de comunicare, vom procesa datele primite in scopul de a raspunde la solicitarea respectiva;
- ca urmare a interactiunii angajatilor nostri cu persoanele vizate (e.g. carti de vizita);
- din surse publice;

6. SCOPURILE SI TEMEIURILE PRELUCRARII

Clinica Dr. Leventer este unul dintre cei mai cunoscuti furnizori privati de servicii de medicina estetica si servicii medicale in specializarea dermatologie din Romania.

Astfel, colectam date cu caracter personal in urmatoarele **scopuri**:

a) Prestarea serviciilor catre pacientii care doresc sa acceseze serviciile Clinicii;
b) Promovarea produselor si serviciilor Clinicii;
c) Executarea contractelor cu furnizorii si partenerii;
d) In procesul de recrutare si gestionare a angajatilor/colaboratorilor nostri;

Colectam date cu caracter personal in urmatoarele **temeiuri**:

a) Consimtamantul persoanelor vizate. In toate cazurile, pentru a accesa serviciile noastre, pacientii completeaza in cadrul Clinicii o serie de formulare care cuprind date cu

caracter personal, furnizarea acestor date echivaland cu un consimtamant si chiar un contract prin care noi prestam servicii. In unele cazuri, consimtamantul va fi considerat acordat prin faptul ca persoana vizata va avea initiativa transmiterii unor date cu caracter personal catre noi, de exemplu, in cazul contactarii societatii din proprie initiativa de catre persoana vizata direct in clinica, telefonic sau prin intermediul adresei de e-mail a Clinicii;

b) Executarea contractelor. Societatea noastra poate oferi servicii si catre persoane juridice, procesand astfel date cu caracter personal in executarea contractelor cu acestia; in orice caz, in executarea contractelor cu furnizorii/partenerii/colaboratorii nostri putem sa procesam date cu caracter ale reprezentantilor sau ale clientilor acestora, in functie de specificul fiecarui contract in parte;

c) Indeplinirea unor obligatii legale;

d) Indeplinirea intereselor legitime ale Clinicii care nu se vor opune drepturilor superioare ale persoanei vizate.

7. DESTINATARI

Clinica nu transfera date cu caracter personal catre destinatari din afara spatiului Uniunii Europene.

Clinica nu vinde, nu ofera si nu pune la dispozitia tertilor in interes comercial datele cu caracter personal pe care le prelucreaza. Clinica poate avea anumite relatii cu parteneri si colaboratori (in special medici), situatie in care este posibil ca anumite date sa fie transferate catre si de la acestia.

Informațiile persoanelor vizate pot fi stocate într-o bază de date din Uniunea Europeana (UE). Clinica isi asuma respectarea confidențialitatii informațiilor personale procesate. Clinica, direct sau prin împuterniciții săi, va procesa datele in calitate de operator de date cu caracter personal, iar aceste date pot fi accesibile și folosite numai de către angajatii/colaboratorii Clinicii, direct sau prin împuterniciții acestora, precum şi de către partenerii contractuali ai Clinicii, direct sau prin împuterniciţii acesteia.

In cazul in care se solicita Clinicii dezvăluirea informațiilor persoanelor vizate printr-un ordin judecătoresc sau pentru a se conforma altor cerințe legale sau de reglementare, societatea va da curs acestor solicitari in conformitate cu prevederile legale in vigoare.

8. DREPTURILE PERSOANELOR VIZATE

Conform GDPR, toate persoanele fizice carora le prelucram date cu caracter personal au drepturi specifice, printre care mentionam:

a) **Dreptul la informare:** dreptul de a afla ce date sunt procesate, scopurile si temeiurile prelucrarii, destinatarii datelor, perioada de stocare, existenta drepturilor persoanelor vizate, dreptul de a se adresa autoritatii de supraveghere etc.;

b) **Dreptul de acces:** dreptul de a obține din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care privesc și, în caz afirmativ, acces la datele respective și la informații privind prelucrarea detaliate anterior;

c) **Dreptul la rectificare**: dreptul de a obtine corectarea datelor inexacte sau completarea datelor lipsa;

d) **Dreptul la stergerea datelor:** dreptul de a solicita stergerea datelor procesate, in situatiile prevazute de lege;

e) **Dreptul de a solicita restrictionarea prelucrarii**, in limitele prevazute de lege.

f) **Alte drepturi** care pot fi exercitate in limitele prevazute de lege: dreptul la portabilitatea datelor, dreptul de a obiecta la prelucrarea datelor, dreptul de a se opune proceselor decizionale automate, dreptul de a se adresa autoritatilor competente cu solicitari privind prelucrarile efectuate de Clinica etc.

9. SECURITATEA DATELOR COLECTATE

In conformitate cu prevederile legale in vigoare si cu stadiul actual al tehnologiei, Clinica a implementat masuri tehnice si organizatorice adecvate pentru asigurarea securitatii datelor cu caracter personal in decursul activitatii noastre, conform regulilor detaliate mai jos. Am actualizat formularistica utilizata in cadrul Clinicii pentru a ne asigura ca intotdeauna persoanele vizate, in special pacientii, sunt permanent informati cu privire la procesarile pe care le efectuam si sunt la curent cu drepturile lor.

In activitatea noastra urmarim in primul rand prevenirea oricaror incidente de securitate, precum acces neautorizat la date, scurgeri de informatii, stergere accidentala a datelor si altele asemenea, intreaga structura prelucrarilor de date fiind construita in jurul principiului preventiei.

Totusi, avand in vedere ca in societatea informationala securitatea prelucrarilor nu poate fi 100% garantata, Clinica a luat, de asemenea, masuri ca, in cazul improbabil in care apar incidente de securitate, intinderea si gravitatea acestora sa fie diminuate.

Avand in vedere ca unele dintre informatiile colectate pot avea caracter sensibil (in special datele de sanatate colectate), ne asumam impunerea unor standarde suplimentare de securitate pentru aceste informatii.

10. REGULI GENERALE

Pentru a asigura protectia adecvata a datelor cu caracter personal la care Clinica are acces, am implementat masuri organizatorice si tehnice, precum:

a) Semnarea unor documente suplimentare cu angajatii, colaboratorii si partenerii nostri pentru asigurarea confidentialitatii datelor cu caracter personal la care au acces cel putin la un nivel similar cu cel impus de compania noastra.

b) Implementarea unor masuri de securitate fizice cu privire la documentele care contin date cu caracter personal, cum ar fi, de exemplu, stocarea documentelor in dulapuri inchise cu cheie la care are acces doar personalul autorizat, implementarea unor sisteme de acces restrictionat (de exemplu, chei, carduri de acces) exclusiv pentru persoanele care justifica un interes pentru accesul respectivelor date.

c) Implementarea unor masuri de securitate in ceea ce priveste sistemele informatice, cum ar fi, de exemplu, asigurarea ca toate echipamentele noastre dispun de programe de securitate corespunzatoare, asigurarea unor copii de rezerva etc.

d) Implementarea unor programe de instruire a personalului cu privire la cerintele GDPR.

11. REGULI SPECIFICE

Clinica a implementat urmatoarele reguli specifice pentru protectia datelor cu caracter personal:

a) **Reguli de securitate tehnica**

i. Interzicerea folosirii de catre utilizatorii de sisteme a unor programe software nelicentiate sau care provin din surse nesigure;

ii. Implementarea unui sistem de autentificare bazat pe user si parole securizate, unice pentru fiecare utilizator autorizat; astfel, pe de o parte se impiedica accesul tertilor la terminale / bazele de date si, pe de alta parte, la introducerea gresita a userului / parolei de un anumit numar de ori, sistemul se blocheaza automat, conform procedurilor tehnice interne;

iii. Implementarea unor masuri de securitate adecvate ale echipamentelor IT si software-ului utilizat in activitatea noastra, dupa cum urmeaza:

- informarea utilizatorilor in privinta pericolului privind virusii informatici;
- implementarea unor software-uri de protectie adecvate pe terminalele utilizate, precum programe antivirus si informarea salariatilor asupra obligativitatii de scanare periodica a sistemelor pentru prevenirea oricaror programe neautorizate (e.g. malware, phishing) sau, dupa caz, implementarea unor sisteme automate de devirusare si de securitate a sistemelor informatice;
- dezactivarea pe cat posibil tastei "*Print screen*", atunci cand sunt afisate pe monitor date cu caracter personal, limitandu-se astfel posibilitatea de scoatere

la imprimanta a acestora de catre alti utilizatori decat aceia autorizati in acest sens;

- limitarea drepturilor de printare, prin implementarea unor sisteme bazate pe user / parola;
- monitorizarea accesului la baza de date si logarea accesului si a parcursului utilizatorului;
- schimbarea periodica a parolelor de acces la baza de date si la sistemele informatice;
- obligatia angajatilor de a securiza accesul in terminalele proprii atunci cand nu le utilizeaza si de a inchide terminalele la finalul programului de munca;
- limitarea drepturilor de acces la bazele de date de la distanta (i.e. din afara firmei) / cu utilizarea altor dispozitive decat cele puse la dispozitie de societate;
- interzicerea utilizarii unor retele publice (cu acces deschis) de conexiune la internet.

b) **Reguli de securitate organizatorica**

i. Limitarea numarului de destinatari / utilizatori care au acces la datele cu caracter personal si corelarea drepturilor de acces cu necesitatea justificata de fiecare utilizator – e.g. prin impartirea pe arii geografice a informatiilor despre persoanele vizate, prin transmiterea catre imputerniciti doar a datelor necesare pentru executarea contractului etc.;

ii. Introducerea unor conditii si obligatii de confidentialitate si protectie a datelor cu caracter personal suplimentare pentru angajati, colaboratori, furnizori si parteneri;

iii. Introducerea unor reguli specifice privind copierea si diseminarea documentelor pentru a preveni raspandirea si accesul unor persoane neautorizate la datele cu caracter personal;

iv. Introducerea unor reguli prin care angajatii, colaboratorii si partenerii nostri au acces numai la acele date cu caracter personal necesare indeplinirii fisei postului sau, dupa caz, a obligatiilor asumate fata de Clinica;

v. Instalarea unor sisteme de alarma si monitorizare a accesului in spatiile unde sunt stocate documentele care contin date cu caracter personal sau echipamentele pe care sunt stocate aceste date de catre proprietarul cladirii in care ne desfasuram activitatea;

vi. Instalarea unor sisteme de asigurare a securitatii fizice a documentelor care cuprind date cu caracter personal, precum dulapuri inchise sub cheie, asigurarea supravegherii video a cladirii in care ne desfasuram activitatea (fiind marcate

corespunzator zonele supravegheate video) de catre proprietarul cladirii in care ne desfasuram activitatea;

vii. Realizarea unor copii de siguranta a datelor stocate;

viii. Restrictionarea accesului persoanelor neautorizate in spatiile unde sunt stocate datele cu caracter personal sau echipamentele pe care acestea sunt stocate, decat cu asigurarea unor conditii de confidentialitate corespunzatoare;

ix. Interzicerea copierii datelor cu caracter personal pe medii de stocare mobile, fara acordul prealabil al conducerii societatii, cu exceptia situatiei cand aceasta este necesara pentru indeplinirea unor obligatii asumate contractual fata de clienti;

x. Asigurarea instruirii periodice a personalului cu privire la cerintele GDPR, precum si cele de securitate si riscurile privind datele cu caracter personal.

12. DISPOZITII FINALE

Pentru mai multe detalii, informatii si solicitari orice persoana interesata se poate adresa printr-un e-mail la adresa dedicata contact@drleventercentre.com, prin telefon la numarul 0722 363 577 sau 021 310 65 07 sau direct la sediul nostru din Str. Monetăriei nr. 8, sector 1, 011216, București. Pentru exercitarea anumitor drepturi ne rezervam dreptul de a solicita ca cererea sa fie depusa in scris, semnata de persoana vizata si ca solicitantul sa prezinte dovezi suficiente de identificare cu persoana vizata (care exercita dreptul conferit de lege).