

POLITICA DE SECURITATE A PRELUCRĂRII DATELOR CU CARACTER PERSONAL A SOCIETĂȚII

SAN MED 2001 S.R.L.

Prezenta politică de securitate a fost creată având în vedere:

- Faptul că S.C. **SAN MED 2001 S.R.L.**, cu sediul social în București, str. G-ral Petre Popovăț, nr. 15, sector 6, înregistrată la Oficiul Registrului Comerțului București, sub nr. 10256 din 13.12.2014, cod fiscal nr. 14348421 din 13.12.2014, reprezentată de Zamescu Georgeta, cu funcția de administrator (denumită în continuare “**San Med**” sau “**Noi**”) desfășoară o activitate care presupune procesarea unor categorii de date cu caracter personal,
- intrarea în vigoare începând 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 în continuare “**GDPR**”),
- obligația impusă de GDPR de a asigura măsuri de securitate tehnice și organizatorice adecvate tuturor activităților de procesare a datelor cu caracter personal.

1. ANGAJAMENT

San Med prelucrează date cu caracter personal în scopuri legitime, cu respectarea tuturor principiilor impuse de GDPR și de practicile comerciale etice. Protejarea siguranței și securității datelor personale este importantă pentru San Med și această politică descrie cadrul organizatoric implementat pentru asigurarea conformității prelucrării.

Obiectivul principal al acestei Politici de Securitate este de a contribui la desfășurarea activității societății cu respectarea prevederilor legale specifice și de a minimiza riscurile prin prevenirea incidentelor și, în cazul imprevizibil al unor astfel de incidente, reducerea impactului lor asupra persoanei vizate.

Ne propunem să avem o relație bazată pe încredere, transparență, bună-credință și etică în relația cu toți partenerii, colaboratorii și angajații noștri.

2. DEFINIȚII

“**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 (cărui) 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

San Med 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 San Med se face in scopuri determinate, explicite si legitime si nu sunt prelucrate ulterior intr-un mod incompatibil cu aceste scopuri;

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

- **Limitare prin raportare la scop** – San Med 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** – San Med pastreaza datele persoanelor vizate pe o perioada care nu depaseste perioada necesara indeplinirii scopurilor in care sunt prelucrate datele, precum si pe perioada prevazute de lege (de exemplu, prin normele Casei Nationale de Asigurari de Sanatate);

- **Exactitate si acuratete** – San Med 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** – San Med 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

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

- Pacienti – datele de identificare si orice alte date de sanatate colectate in cadrul furnizarii serviciilor medicale;
- Angajatii furnizorilor societatii;
- Angajatii proprii;
- Dupa caz, alte persoane fizice care interactioneaza cu societatea in cursul activitatii acesteia.

5. DATELE COLECTATE

In functie de specificul fiecarei relatii, San Med 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 profesionale: loc de munca, pozitie, vechime, experienta profesionala;
- Date colectate despre angajati si familiile acestora, in scopul respectarii contractului de munca si a prevederilor legale in domeniul muncii;
- Vocea si imaginea persoanelor vizate, in cazul monitorizarii audio-video a spatiilor societatii;
- Date furnizate direct prin e-mail sau prin alte modalitati de catre persoanele vizate;
- Date de sanatate;

Datele cu caracter personale mentionate mai sus au caracter exemplificativ.

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

- De la pacienti, ca urmare a furnizarii serviciilor contractate;
- Din contracte si documente auxiliare acestora, inclusiv in executarea relatiilor de munca;

- Ca urmare a furnizarii acestora direct de catre persoana vizata – cu obtinerea consimtamantului in cazurile prevazute de lege;
- De la furnizori, in functie de activitatea propriu zisa (de exemplu, datele de contact ale persoanelor care livreaza produse catre San Med);
- Date colectate in mod pasiv (de exemplu, prin sistemele de monitorizare audio-video);

6. SCOPURILE SI TEMEIURILE PRELUCRARI

San Med este o societate avand ca obiect de activitate principal furnizarea de servicii medicale de familie sau specializate

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

- a) Executarea contractelor. Societatea noastra ofera servicii medicale catre persoane fizice, inclusiv in executarea contractelor incheiate cu Casa de Asigurari de Sanatate. In cadrul acestor operatiuni, se colecteaza date cu caracter personal necesare furnizarii serviciilor, inclusiv date de sanatate ale pacientilor; de asemenea, procesam datele cu caracter personal ale angajatilor societatii, in vederea executarii contractelor de munca;
- b) Consimtamantul persoanelor vizate. 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 prin intermediul formularului de contact de pe website-ul San Med;
- c) Indeplinirea unor obligatii legale, in special in relatia cu Casele de Asigurari de Sanatate;
- d) Indeplinirea intereselor legitime ale San Med care nu se vor opune drepturilor superioare ale persoanei vizate.

7. DESTINATARI

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

San Med nu vinde, nu ofera si nu pune la dispozitia tertilor in interes comercial datele cu caracter personal pe care le prelucreaza.

Informațiile persoanelor vizate pot fi stocate într-o bază de date din Uniunea Europeană (UE). San Med își asumă respectarea confidențialității informațiilor personale procesate. San Med, direct sau prin împuterniciții săi, va procesa datele în calitate de operator de date cu caracter personal, iar aceste date pot fi accesibile și folosite numai de către angajații San Med, direct sau prin împuterniciții acestora, precum și de către partenerii contractuali ai San Med (de exemplu, furnizori de servicii IT, furnizori de servicii de laborator sau furnizori de servicii specifice relațiilor de muncă), direct sau prin împuterniciții acestora.

În cazul în care se solicită San Med dezvăluirea informațiilor persoanelor vizate printr-un ordin judecătoresc sau pentru a se conforma altor cerințe legale sau de reglementare, societatea va da curs acestor solicitări în conformitate cu prevederile legale în vigoare.

8. DREPTURILE PERSOANELOR VIZATE

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

- a) **Dreptul la informare:** dreptul de a afla ce date sunt procesate, scopurile și temeiurile prelucrării, destinatarii datelor, perioada de stocare, existența drepturilor persoanelor vizate, dreptul de a se adresa autorității 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 le privesc și, în caz afirmativ, acces la datele respective și la informații privind prelucrarea detaliată anterior;
- c) **Dreptul la rectificare:** dreptul de a obține corectarea datelor inexacte sau completarea datelor lipsă;
- d) **Dreptul la ștergerea datelor:** dreptul de a solicita ștergerea datelor procesate, în situațiile prevăzute de lege;
- e) **Dreptul de a solicita restricționarea prelucrării,** în limitele prevăzute de lege.
- f) **Alte drepturi** care pot fi exercitate în limitele prevăzute 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 autorităților competente cu solicitări privind prelucrările efectuate de San Med etc., dreptul de a retrage consimțământul, în orice moment, pentru prelucrarea datelor personale pentru care temeiul prelucrării îl reprezintă consimțământul persoanei vizate.

9. SECURITATEA DATELOR COLECTATE

In conformitate cu prevederile legale in vigoare si cu stadiul actual al tehnologiei, San Med a implementat si implementeaza in permanenta masuri tehnice si organizatorice adecvate pentru asigurarea securitatii datelor cu caracter personal in decursul activitatii noastre, conform regulilor detaliate mai jos.

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 a prelucrarilor de date fiind construita in jurul principiului preventiei.

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

In cazul aparitiei unor incidente de securitate, persoanele vizate vor fi notificate fara intarziere cu privire la aceasta.

10. REGULI GENERALE

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

- a) Semnarea unor documente suplimentare cu angajatii si furnizorii 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, spatiile unde se stocheaza date cu caracter personal sunt securizate cu ajutorul unei firme de paza si sunt accesibile personalului autorizat doar cu cheie) 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 notificare a personalului cu privire la cerintele GDPR.

11. REGULI SPECIFICE

San Med 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;
 - 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 San Med;
- v. Instalarea unor sisteme de alarma si monitorizare audio-video a accesului in spatiile unde sunt stocate documentele care contin date cu caracter personal sau echipamentele pe care sunt stocate aceste date;
- vi. Instalarea unor sisteme de asigurare a securitatii fizice a documentelor care cuprind date cu caracter personal, precum dulapuri inchise sub cheie, asigurarea supravegheerii video a cladirii in care ne desfasuram activitatea (fiind marcate corespunzator zonele supravegheate video) si a cladirilor administrate de noi;
- vii. Realizarea unor copii de siguranta ale 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 noastra sanmed2001@yahoo.com sau direct la sediul nostru din Str. Petre Popovat nr. 15, Sector 6, Bucuresti. 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).