ACORD DE PRELUCRARE A DATELOR CU CARACTER PERSONAL

Data Processing Agreement (DPA)

conform Art. 28 din Regulamentul (UE) 2016/679 (GDPR) și Legii nr. 190/2018

Versiunea 3.3 · 16.06.2026

PREAMBUL

Prezentul Acord de Prelucrare a Datelor cu Caracter Personal ("DPA") este încheiat între:

OPERATORUL DE DATE	PERSOANA ÎMPUTERNICITĂ
Cabinetul stomatologic / Utilizatorul Persoana juridică sau fizică autorizată care activează în domeniul serviciilor stomatologice și utilizează Platforma VAstoma în baza unui contract de abonament. Calitate GDPR: Operator de date (Art. 4(7) GDPR) Confirmare: Utilizatorul care acceptă prezentul DPA declară că are autoritatea de a angaja juridic Operatorul (administrator, medic titular sau persoana desemnată).	WELIST S.R.L. CUI: 54493544 · Iași, România contact@vastoma.ro · gdpr@vastoma.ro security@vastoma.ro · vastoma.ro Calitate GDPR: Persoană împuternicită (Art. 4(8) și Art. 28 GDPR) — prelucrează datele exclusiv în numele și la instrucțiunile Operatorului.

ARTICOLUL 1 — DEFINIȚII

„Date cu Caracter Personal": Orice informații referitoare la o persoană fizică identificată sau identificabilă, în sensul Art. 4(1) GDPR.

„Date de Sănătate": Date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, în sensul Art. 4(15) GDPR. Constituie categorie specială conform Art. 9 GDPR și beneficiază de protecție sporită.

„Instrucțiuni documentate": Instrucțiunile explicite și implicite ale Operatorului privind prelucrarea datelor, incluzând configurările Platformei, prezentul DPA și contractul de abonament, conform Art. 28(3)(a) GDPR.

„Persoană Vizată": Pacientul cabinetului stomatologic sau orice persoană fizică ale cărei date sunt prelucrate prin Platforma VAstoma.

„Sub-Procesator": Orice terț angajat de WELIST S.R.L. care prelucrează date în calitate de subcontractant, conform Art. 28(2) GDPR.

„Breșă de Securitate": O încălcare care conduce la distrugerea, pierderea, modificarea sau accesul neautorizat la date, în sensul Art. 4(12) GDPR.

„Platforma VAstoma": Ansamblul de servicii software sub marca VAstoma: agentul AI WhatsApp, dashboard-ul de gestionare a programărilor și componentele asociate.

„TOM": Măsuri Tehnice și Organizatorice implementate de WELIST S.R.L. pentru protecția datelor, detaliate în Anexa II.

„DPIA": Evaluare a Impactului asupra Protecției Datelor, conform Art. 35 GDPR.

„ANSPDCP": Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, România.

ARTICOLUL 2 — OBIECTUL, DURATA ȘI INSTRUCȚIUNILE DOCUMENTATE

2.1 Obiect

WELIST S.R.L. prelucrează Date cu Caracter Personal exclusiv în scopul furnizării serviciilor Platformei VAstoma:

• Gestionarea automată a programărilor stomatologice prin agentul AI WhatsApp

• Stocarea și afișarea istoricului programărilor în dashboard-ul web

• Trimiterea de notificări și remindere automate către pacienți

• Gestionarea listei de așteptare pentru servicii stomatologice

• Generarea de rapoarte statistice lunare pentru cabinet

• Integrarea opțională cu Google Calendar (activată explicit de Operator)

2.2 Instrucțiunile documentate ale Operatorului (Art. 28(3)(a) GDPR)

WELIST prelucrează date exclusiv pe baza instrucțiunilor documentate ale Operatorului, care includ:

• Gestionarea și confirmarea programărilor solicitate prin WhatsApp

• Transmiterea de remindere automate cu 24 ore înainte de programare

• Stocarea istoricului conversațiilor pe durata contractului, pentru continuitatea serviciului

• Sincronizarea programărilor în Google Calendar al cabinetului (dacă activată)

• Generarea rapoartelor lunare cu programările și veniturile cabinetului

• Trimiterea notificărilor de disponibilitate pentru pacienții din lista de așteptare

• Orice altă instrucțiune transmisă în scris prin platforma de administrare

WELIST va informa imediat Operatorul dacă o instrucțiune primită încalcă GDPR sau altă reglementare aplicabilă.

2.3 Durata și ștergerea datelor

Prezentul Acord rămâne în vigoare pe toată durata contractului de abonament. La încetarea contractului:
(a) Datele sunt eliminate din sistemele active fără întârzieri nejustificate, cel târziu în 30 de zile calendaristice;
(b) Datele expiră din copiile de siguranță (backup-uri) conform ciclului normal de retenție, care nu depășește 90 de zile de la ultimul backup. Ștergerea din backup-uri se realizează prin ciclul de retenție, nu prin ștergere granulară — practică standard SaaS;
(c) Operatorul poate solicita exportul datelor în format CSV/JSON în primele 14 zile de la încetare.

Notă: Pe durata contractului, cache-ul temporar al agentului AI (contextul conversației) este șters automat după 90 de zile de inactivitate, fără a afecta istoricul programărilor salvat în dashboard-ul Operatorului, care se păstrează pe toată durata contractului.

ARTICOLUL 3 — NATURA, SCOPUL ȘI TEMEIUL LEGAL AL PRELUCRĂRII

3.1 Categorii de date prelucrate

Categorie date	Exemple concrete	Sub-procesator	Temei legal
Date identificare pacient	Nume, prenume, număr WhatsApp	Twilio, Meta WA API	Art. 6(1)(b) GDPR
Date programare	Data, ora, serviciu, status	Hetzner, Google Calendar (opț.)	Art. 6(1)(b) GDPR
Conținut conversații WhatsApp	Mesaje schimbate pentru gestionarea programării	Anthropic, Twilio, Meta WA API	Art. 6(1)(b) GDPR
Date de sănătate menționate spontan (Art. 9 GDPR)	Informații medicale menționate din proprie inițiativă de pacient în conversație (ex: alergii, tratamente). Nu solicitate activ de platformă.	Hetzner (stocare), Anthropic (procesare NLP)	Art. 9(2)(h) GDPR — sub responsabilitatea medicului stomatolog, profesionist cu secret profesional
Observații medicale introduse de medic	Note clinice, alergii, tratamente introduse manual în dashboard	Hetzner	Art. 9(2)(h) GDPR — sub responsabilitatea medicului
Date istorice programări	Istoric vizite, servicii efectuate	Hetzner	Art. 6(1)(f) GDPR — interes legitim
Loguri tehnice	IP, timestamp (fără conținut personal)	Cloudflare, Hetzner	Art. 6(1)(f) GDPR — securitate

⚠ DATE DE SĂNĂTATE — NOTĂ ART. 9 GDPR

Platforma VAstoma este un instrument administrativ pentru gestionarea programărilor stomatologice și nu solicită în mod activ date medicale de la pacienți. Nu există câmpuri sau fluxuri destinate colectării de informații medicale prin WhatsApp.

Cu toate acestea, în mod ocazional și nesolicitat, pacienții pot menționa din proprie inițiativă informații legate de starea lor de sănătate în cadrul conversației. Aceste informații sunt procesate incidental, în temeiul Art. 9(2)(h) GDPR, exclusiv sub responsabilitatea medicului stomatolog — profesionist supus secretului profesional conform legislației române.

WELIST S.R.L. transmite conținutul conversației către Anthropic API pentru generarea răspunsului AI. Conform documentației contractuale publicate de Anthropic, datele transmise prin API nu sunt utilizate pentru antrenarea modelelor. WELIST limitează transmiterea datelor la minimul necesar funcționării serviciului și evaluează continuu posibilitatea extinderii măsurilor de minimizare.

Obligația Operatorului: Cabinetul are obligația de a nu solicita activ informații medicale detaliate prin intermediul agentului AI WhatsApp și de a informa pacienții despre această posibilitate prin propria politică de confidențialitate.

3.2 DPIA — Evaluarea Impactului

WELIST S.R.L. a efectuat o Evaluare a Impactului (DPIA) internă privind funcționalitățile AI, datele de sănătate și transferurile internaționale. WELIST va reevalua periodic riscurile, cel puțin anual sau la schimbări semnificative, și va asista Operatorul în realizarea propriei DPIA dacă este necesară conform Art. 35 GDPR.

3.3 Utilizarea Agentului AI

Scop exclusiv administrativ: Agentul AI VAstoma furnizează suport administrativ pentru gestionarea programărilor stomatologice și nu oferă recomandări medicale, diagnostic sau tratament de nicio natură.

Interdicție profilare: WELIST nu utilizează Platforma pentru crearea de profiluri comportamentale sau medicale ale pacienților și nu aplică decizii automate cu efecte juridice asupra Persoanelor Vizate, conform Art. 22 GDPR.

Urgențe medicale: Agentul AI direcționează pacienții care menționează simptome de urgență să contacteze cabinetul medical sau serviciul de urgențe 112.

ARTICOLUL 4 — OBLIGAȚIILE PERSOANEI ÎMPUTERNICITE (WELIST S.R.L.)

4.1 Prelucrare pe baza instrucțiunilor

WELIST prelucrează date exclusiv pe baza instrucțiunilor documentate din Art. 2.2 și va informa imediat Operatorul dacă o instrucțiune încalcă GDPR.

4.2 Confidențialitate

Persoanele autorizate să acceseze date au semnat angajamente de confidențialitate. Accesul este limitat la personalul cu nevoie demonstrată (principiul need-to-know).

4.3 Măsuri tehnice și organizatorice (Art. 32 GDPR)

WELIST implementează un set integrat de TOM-uri detaliate în Anexa II, care include măsuri de securitate a rețelei, criptare, control acces, backup și management al vulnerabilităților. Utilizarea WhatsApp Business API oficial (nu WhatsApp consumer) face parte din acest set de măsuri tehnice, în concordanță cu recomandările publice ale ANSPDCP privind utilizarea canalelor de comunicare electronică.

4.4 Sub-procesatori (Art. 28(4) GDPR)

WELIST utilizează exclusiv sub-procesatorii autorizați din Art. 6 și le impune obligații echivalente prin contracte separate. WELIST rămâne pe deplin răspunzătoare față de Operator pentru executarea obligațiilor sub-procesatorilor, conform Art. 28(4) GDPR.

4.5 Asistarea Operatorului

WELIST asistă Operatorul în: răspunsul la cererile GDPR (Art. 15-22), realizarea DPIA-urilor și consultările prealabile cu ANSPDCP conform Art. 36 GDPR.

4.6 Notificarea breșelor de securitate

WELIST notifică Operatorul în maximum 24 de ore de la identificarea unei Breșe de Securitate, furnizând informațiile necesare pentru notificarea ANSPDCP în termenul de 72 ore (Art. 33 GDPR). Contact urgențe: security@vastoma.ro.

4.7 Ștergerea datelor

WELIST șterge datele conform Art. 2.3 și furnizează la cerere confirmare scrisă a ștergerii din sistemele active.

4.8 Auditare

WELIST permite audituri cu notificare de minimum 14 zile și pune la dispoziție informațiile necesare pentru demonstrarea conformității cu Art. 28 GDPR.

ARTICOLUL 5 — OBLIGAȚIILE OPERATORULUI (CABINETUL STOMATOLOGIC)

5.1. Să informeze Persoanele Vizate (pacienții) despre prelucrarea datelor prin Platforma VAstoma, inclusiv utilizarea agentului AI WhatsApp, înainte de inițierea primului contact, prin propriile politici de confidențialitate;

5.2. Să asigure un temei legal valabil pentru prelucrarea datelor, inclusiv a Datelor de Sănătate, conform Art. 6 și Art. 9 GDPR;

5.3. Să nu solicite activ pacienților date medicale detaliate prin conversațiile WhatsApp, dincolo de ce este strict necesar pentru gestionarea programărilor;

5.4. Să efectueze propria analiză privind obligativitatea desemnării unui DPO conform Art. 37 GDPR și, dacă este cazul, să îl înregistreze la ANSPDCP;

5.5. Să notifice ANSPDCP prelucrările de date de sănătate efectuate în calitate de Operator, conform Legii 190/2018, cu excepția cazului în care a desemnat un DPO înregistrat la ANSPDCP;

5.6. Să notifice WELIST S.R.L. orice exercitare a drepturilor GDPR de către Persoanele Vizate în termen de 5 zile lucrătoare;

5.7. Să notifice ANSPDCP orice Breșă de Securitate în termen de 72 de ore, conform Art. 33 GDPR, pe baza informațiilor furnizate de WELIST;

5.8. Să securizeze credențialele de acces și să notifice imediat WELIST orice acces neautorizat suspectat;

5.9. Să confirme că utilizatorul care acceptă DPA-ul are autoritatea de a angaja juridic Operatorul.

ARTICOLUL 6 — SUB-PROCESATORI AUTORIZAȚI

Operatorul autorizează utilizarea următorilor sub-procesatori. WELIST rămâne pe deplin răspunzătoare (Art. 28(4) GDPR). TIA-urile sunt disponibile la gdpr@vastoma.ro și actualizate anual:

Sub-procesator	Locație	Scop prelucrare	Categorii date	Transfer SUA
Hetzner Online GmbH	Germania (UE)	Hosting server, stocare date	Toate categoriile (stocare)	Nu — UE
Cloudflare Inc.	SUA/UE	CDN, protecție DDoS, WAF, geo-blocking	IP, loguri tehnice (fără conținut conversații)	Da — DPF + SCC
Meta Platforms Ireland Ltd. (WhatsApp Business API oficial)	Irlanda (UE)	Transmitere mesaje WhatsApp. API oficial — distinct de WhatsApp consumer.	Număr telefon, conținut mesaje WhatsApp	Da — DPF + SCC
Anthropic PBC (Claude API)	SUA	Procesare NLP pentru răspunsuri AI. Conform documentației contractuale Anthropic: nu antrenează modele pe date API; retenție minimă tehnică pentru detecție abuzuri.	Conținut conversații (incl. posibil info medicale spontane nesolicitate)	Da — SCC (Dec. 2021/914, Modul 2) + TIA
Twilio Inc.	SUA	Gateway WhatsApp Business API, apeluri vocale reminder	Număr telefon, conținut mesaje, text reminder vocal	Da — DPF + SCC
Stripe Inc.	Irlanda (UE)	Procesare plăți abonamente. Nu procesează date pacienți.	Date facturare cabinet exclusiv	Da — SCC
Resend Inc.	SUA	Emailuri tranzacționale sistem. Notificările pot conține date minime de programare.	Email cabinet; posibil date minime programare	Da — SCC
ElevenLabs Inc.	SUA	Generare voce sintetică pentru remindere vocale	Text reminder (poate include prenume pacient și oră programare)	Da — SCC
Google LLC (Calendar API — opțional)	SUA/UE	Sincronizare programări în Google Calendar al cabinetului. Activat explicit de cabinet. Calendarul aparține cabinetului.	Data, ora, serviciu programare	Da — DPF + SCC
UptimeRobot Ltd.	SUA	Monitorizare disponibilitate. Nu procesează date pacienți.	URL platformă, status HTTP (fără date personale)	Da — SCC

Notificare schimbare sub-procesatori: WELIST notifică Operatorul cu minimum 30 de zile înainte de orice modificare, acordând dreptul de opoziție.

ARTICOLUL 7 — TRANSFERURI INTERNAȚIONALE DE DATE

Transferurile în afara SEE se realizează exclusiv prin mecanismele prevăzute de Capitolul V GDPR: (a) Clauze Contractuale Standard (SCC) — WELIST S.R.L. garantează că transferurile către sub-procesatorii din SUA sunt reglementate prin SCC încheiate direct între WELIST S.R.L. și aceștia, conform Deciziei 2021/914/UE, Modulul 2 sau Modulul 3, după caz. Operatorul poate solicita copii la gdpr@vastoma.ro; (b) EU-US Data Privacy Framework (DPF) — pentru sub-procesatorii certificați; (c) TIA — efectuate și actualizate anual pentru toți sub-procesatorii din SUA, disponibile la solicitare la gdpr@vastoma.ro.

ARTICOLUL 8 — EXERCITAREA DREPTURILOR PERSOANELOR VIZATE

Dreptul	Termen WELIST	Modalitate
Acces (Art. 15)	5 zile lucrătoare	Export CSV cu datele pacientului
Rectificare (Art. 16)	3 zile lucrătoare	Corectare directă în baza de date
Ștergere (Art. 17)	5 zile lucrătoare	Ștergere sisteme active; backup-uri la ciclul de retenție
Portabilitate (Art. 20)	7 zile lucrătoare	Export JSON sau CSV structurat
Restricționare (Art. 18)	3 zile lucrătoare	Marcare date ca restricționate
Opoziție (Art. 21)	3 zile lucrătoare	Oprire prelucrare automată, notificare Operator

ARTICOLUL 9 — PROCEDURA DE GESTIONARE A BREȘELOR DE SECURITATE

 TIMELINE OBLIGATORIU — BREȘĂ DE SECURITATE

Ora 0: WELIST identifică sau este notificată despre breșă
Max. 24 ore: WELIST notifică Operatorul — natura breșei, categorii date, număr persoane afectate, consecințe probabile, măsuri luate
Max. 72 ore: Operatorul notifică ANSPDCP (dataprotection.ro — formular online)
Dacă risc ridicat: Operatorul notifică Persoanele Vizate afectate (Art. 34 GDPR)
30 zile: WELIST transmite raport complet de investigație

Contact urgențe 24/7: security@vastoma.ro

ARTICOLUL 10 — EVALUAREA OBLIGATIVITĂȚII DESEMNĂRII DPO

10.1 WELIST S.R.L.

WELIST S.R.L. a efectuat evaluarea obligativității desemnării unui DPO conform Art. 37 GDPR. În prezent, prelucrarea categoriilor speciale de date se realizează exclusiv în calitate de persoană împuternicită (nu ca operator principal), iar volumul curent nu se încadrează în criteriile de „scară largă" din Art. 37(1)(c) GDPR. WELIST va reevalua această obligație cel puțin anual sau la schimbări semnificative ale prelucrărilor. Punct de contact GDPR: gdpr@vastoma.ro.

10.2 Operatorul (cabinetul stomatologic)

Fiecare cabinet stomatologic trebuie să efectueze propria analiză privind obligativitatea desemnării unui DPO conform Art. 37 GDPR și, dacă este cazul, să îl înregistreze la ANSPDCP prin formularul disponibil la dataprotection.ro.

ARTICOLUL 11 — RĂSPUNDERE ȘI ALOCAREA RISCULUI

11.1 Responsabilități Operator: Operatorul răspunde pentru: (a) temeiul legal al prelucrării; (b) informarea pacienților; (c) conținutul datelor introduse; (d) deciziile medicale; (e) conformitatea cu legislația medicală și secretul medical.

11.2 Responsabilități WELIST: WELIST răspunde pentru: (a) respectarea instrucțiunilor documentate; (b) implementarea TOM-urilor din Anexa II; (c) gestionarea sub-procesatorilor (Art. 28(4) GDPR); (d) notificarea breșelor în termenele prevăzute.

11.3 Limitarea răspunderii: Răspunderea WELIST față de Operator pentru încălcarea prezentului DPA este limitată la valoarea abonamentului plătit în ultimele 12 luni. Această limitare NU se aplică în cazul: (a) intenției sau fraudei; (b) neglijenței grave în implementarea măsurilor de securitate; (c) încălcărilor deliberate ale obligațiilor de confidențialitate; (d) încălcărilor Art. 28(4) GDPR privind sub-procesatorii; (e) amenzilor GDPR aplicate direct WELIST de ANSPDCP sau altă autoritate competentă.

11.4 Clauza AI: Agentul AI VAstoma furnizează exclusiv suport administrativ pentru programări și nu oferă recomandări medicale, diagnostic sau tratament. WELIST nu răspunde pentru prejudicii operaționale sau medicale cauzate de răspunsuri inexacte ale agentului AI (halucinații), atunci când Operatorul nu a confirmat manual programările critice, fără a aduce atingere obligațiilor imperative ale WELIST privind securitatea datelor conform Art. 32 GDPR. Dacă o eroare AI constituie Breșă de Securitate, se aplică procedura din Articolul 9.

ARTICOLUL 12 — MODIFICĂRI

WELIST poate modifica prezentul DPA cu notificare de minimum 30 de zile calendaristice. Continuarea utilizării Platformei constituie acceptarea modificărilor. Versiunile anterioare sunt disponibile la contact@vastoma.ro.

ARTICOLUL 13 — LEGEA APLICABILĂ ȘI JURISDICȚIA

Prezentul DPA este guvernat de legislația română și Regulamentul (UE) 2016/679. Litigiile se soluționează pe cale amiabilă în 30 de zile, apoi prin instanțele competente din Iași, România. Autoritate supraveghere: ANSPDCP, B-dul G-ral Gheorghe Magheru 28-30, Sector 1, București, dataprotection.ro.

ACCEPTARE CONTRACTUALĂ ELECTRONICĂ

Prezentul DPA este acceptat în format electronic prin bifarea opțiunii corespunzătoare în Platforma VAstoma și/sau la prima autentificare în cont. WELIST S.R.L. păstrează logurile electronice care atestă data, ora și adresa IP de pe care a fost exprimat acordul, în scopuri de audit.

Prin acceptare, Operatorul confirmă că: (a) a citit și înțeles prezentul DPA; (b) utilizatorul care acceptă are autoritatea de a angaja juridic Operatorul; (c) acceptă toate obligațiile prevăzute în prezentul DPA.

Acceptarea electronică documentată prin loguri de audit constituie dovadă a acordului contractual în conformitate cu Legea nr. 455/2001 privind semnătura electronică și cu principiile Regulamentului (UE) nr. 910/2014 (eIDAS).

ANEXA I — CLAUZE CONTRACTUALE STANDARD (SCC)

WELIST S.R.L. garantează că transferurile de Date cu Caracter Personal către sub-procesatorii din SUA enumerați în Articolul 6 sunt reglementate prin Clauze Contractuale Standard încheiate direct între WELIST S.R.L. și aceștia, conform Deciziei Comisiei Europene 2021/914/UE, Modulul 2 (operator → împuternicit) sau Modulul 3 (împuternicit → împuternicit), după caz. Operatorul poate solicita copii ale acestor clauze la gdpr@vastoma.ro.

Clauza SCC	Conținut aplicabil
Clauza 8 — Obligații persoană împuternicită	WELIST prelucrează date exclusiv conform instrucțiunilor din prezentul DPA
Clauza 9 — Sub-procesatori	Autorizare generală, notificare 30 zile, lista din Art. 6
Clauza 12 — Răspundere	Operator și WELIST răspund față de persoanele vizate conform Art. 28(4) GDPR
Clauza 13 — Supraveghere	ANSPDCP, B-dul G-ral Gheorghe Magheru 28-30, Sector 1, București
Anexa I SCC — Descriere transfer	Conversații WhatsApp + date programări → Anthropic PBC (SUA) pentru procesare NLP. Temei: Art. 9(2)(h) GDPR. Durata: durata contractului.
Anexa II SCC — TOM	Vezi Anexa II din prezentul DPA

ANEXA II — MĂSURI TEHNICE ȘI ORGANIZATORICE (TOM)

Conform Art. 28(3)(c) și Art. 32 GDPR, WELIST S.R.L. implementează și menține:

1. CONTROLUL ACCESULUI

• Autentificare server exclusiv cu cheie SSH ed25519 (autentificare prin parolă dezactivată)
• Acces la date pacienți limitat la personalul cu nevoie demonstrată (principiul need-to-know)
• Credențiale de administrare separate per persoană, niciodată partajate
• Revizuire anuală a drepturilor de acces
• Dashboard VAstoma: autentificare prin email + parolă cu hashing bcrypt

2. CRIPTARE

• Criptare în tranzit: TLS 1.3 pentru toate conexiunile externe
• Criptare parole utilizatori: bcrypt (cost factor 12)
• Backup-uri criptate stocate pe Hetzner Storage Box
• Comunicații WhatsApp: criptare end-to-end Meta (WhatsApp Business API)

3. SECURITATEA REȚELEI

• Firewall restrictiv pe server (doar porturile strict necesare deschise)
• Fail2ban activ — blocare automată IP-uri după tentative eșuate de autentificare
• Geo-blocking Cloudflare — restricționarea traficului din zone cu risc ridicat
• Rate limiting nginx și Flask-Limiter pentru prevenirea atacurilor automatizate
• WAF Cloudflare pentru filtrarea traficului malițios

4. CONTINUITATE ȘI BACKUP

• Backup zilnic automat al bazei de date și fișierelor de configurare
• Stocare backup pe Hetzner Storage Box (locație geografică separată)
• Testare trimestrială a procesului de restaurare, cu documentarea rezultatelor
• Monitorizare disponibilitate 24/7 cu alerte instantanee

5. MANAGEMENTUL VULNERABILITĂȚILOR

• Actualizări automate de securitate (unattended-upgrades) activate
• Monitorizare loguri de acces zilnic
• Suită extinsă de teste automate și verificări de calitate înainte de lansarea în producție
• Revizuire periodică a dependențelor Python pentru vulnerabilități cunoscute (CVE)

6. GESTIONAREA INCIDENTELOR

• Procedură documentată de răspuns la breșe (Articolul 9 din prezentul DPA)
• Punct de contact securitate: security@vastoma.ro
• Înregistrare și documentare a tuturor incidentelor de securitate
• Revizuire anuală a procedurii de gestionare a incidentelor

7. RETENȚIE ȘI ȘTERGERE DATE

• Ștergerea cache-ului temporar al agentului AI după 90 de zile de inactivitate (fără a afecta istoricul din dashboard)
• Ștergerea datelor din sistemele active în 30 de zile de la încetarea contractului

• Expirarea backup-urilor prin ciclul normal de retenție (max. 90 zile post-contract)
• Loguri de audit pentru operațiunile de ștergere

8. DEZVOLTARE SECURIZATĂ

• Validare input pentru toate câmpurile (prevenire SQL injection, XSS)
• CSRF protection activă pe toate formularele
• HMAC verification pentru webhook-urile Meta și Twilio
• Separare medii: development / production
• Code review și teste automate înainte de lansarea în producție

ANEXA III — REZUMAT PENTRU CLIENT

Pe scurt — Ce facem și ce nu facem cu datele pacienților tăi

 CE FACEM

• Prelucrăm datele pacienților exclusiv pentru a gestiona programările stomatologice prin WhatsApp
• Stocăm datele pe servere în Germania (UE), la Hetzner Online GmbH
• Criptăm toate conexiunile cu TLS 1.3 și parolele cu bcrypt
• Facem backup zilnic al datelor, criptat, în locație separată
• Trimitem remindere automate pacienților cu 24 ore înainte de programare
• Ștergem datele din sistemele active în 30 de zile după încheierea contractului
• Te notificăm în maximum 24 de ore dacă detectăm o breșă de securitate
• Răspundem la cererile GDPR ale pacienților în 3-7 zile lucrătoare
• Monitorizăm platforma 24/7 pentru disponibilitate și securitate

 CE NU FACEM

• NU vindem, închiriem sau transferăm datele pacienților tăi unor terți în afara sub-procesatorilor autorizați din Art. 6
• NU folosim datele pacienților pentru publicitate sau marketing
• NU creăm profiluri comportamentale sau medicale ale pacienților
• NU aplicăm decizii automate cu efecte juridice asupra pacienților
• NU solicităm activ informații medicale detaliate prin conversațiile WhatsApp
• NU oferim diagnostic medical, tratament sau consultații medicale
• NU accesăm datele pacienților în alte scopuri decât furnizarea serviciului
• NU antrenăm modele AI pe datele din conversațiile pacienților tăi (confirmat contractual de Anthropic)
• NU păstrăm datele după încheierea contractului mai mult decât este necesar

 CONTACTE UTILE

Întrebări GDPR generale: gdpr@vastoma.ro
Urgențe de securitate (24/7): security@vastoma.ro
Contact general: contact@vastoma.ro
DPA online: vastoma.ro/dpa
ANSPDCP (autoritate supraveghere): dataprotection.ro
Formular notificare breșă ANSPDCP: dataprotection.ro → Notificare Breșă RGPD