POLITICĂ GDPR
Protecția datelor cu caracter personal

Laboratorul nostru medical se angajează să prelucreze datele cu caracter personal în mod legal, echitabil și transparent, cu respectarea confidențialității informațiilor medicale și a drepturilor persoanelor vizate. Prezenta Politică stabilește principiile, regulile și responsabilitățile aplicabile prelucrărilor de date realizate de laborator, în conformitate cu Regulamentul (UE) 2016/679 (GDPR), legislația națională aplicabilă și principiile SR EN ISO 15189:2023.

Încadrare în SR EN ISO 15189:2023

Politica GDPR susține și completează cerințele SR EN ISO 15189:2023 privind: confidențialitatea (cap. 4.2), cerințele privind pacienții (cap. 4.3), managementul informațiilor și al sistemelor informatice (cap. 7.11), precum și cerințele sistemului de management (cap. 8) privind controlul documentelor și înregistrărilor, gestionarea riscurilor, neconformitățile, acțiunile corective și auditul intern.

Scop și domeniu de aplicare

Prezenta Politică se aplică tuturor prelucrărilor de date cu caracter personal efectuate de laborator, indiferent de suport (hârtie, electronic, audio-video), inclusiv în cadrul activităților pre-analitice, analitice și post-analitice, în relația cu pacienți, clienți, aparținători, medici trimițători, parteneri contractuali, furnizori, personal și colaboratori.

Politica acoperă, fără a se limita la: recoltare și identificare probe, înregistrare în LIS/EMR, emitere și transmitere rapoarte, programări, facturare, relații contractuale, comunicări, arhivare, suport IT și securitate informațională.

Definiții (termeni-cheie)

- date cu caracter personal: orice informație privind o persoană fizică identificată sau identificabilă
- date privind sănătatea și date genetice: categorii speciale de date (art. 9 GDPR)
- persoană vizată: pacientul sau orice altă persoană ale cărei date sunt prelucrate
- operator: laboratorul, în măsura în care stabilește scopurile și mijloacele prelucrării
- persoană împuternicită: furnizor/partener care prelucrează date în numele operatorului (ex.: IT, curier, arhivare)
- încălcare a securității datelor: incident ce conduce la distrugerea, pierderea, alterarea, divulgarea neautorizată sau accesul neautorizat la date

Principii de prelucrare (GDPR art. 5) și angajamente

- Legalitate, echitate și transparență: informăm persoanele vizate și prelucrăm datele numai în temeiuri legale aplicabile
- Limitarea scopului: colectăm datele numai pentru scopuri determinate, explicite și legitime (diagnostic/servicii medicale, obligații legale, contract)
- Minimizarea datelor: solicităm și utilizăm doar datele strict necesare îndeplinirii scopului
- Exactitate: menținem datele actualizate și corectăm fără întârziere datele inexacte
- Limitarea stocării: păstrăm datele pe perioade stabilite legal/contractual; aplicăm reguli de arhivare și eliminare
- Integritate și confidențialitate: aplicăm măsuri tehnice și organizatorice adecvate pentru securitatea datelor
- Responsabilitate (accountability): documentăm conformarea și demonstrăm controalele implementate

Temeiuri legale și scopuri uzuale de prelucrare

În activitatea de laborator medical, prelucrăm date în principal pentru furnizarea serviciilor medicale și emiterea rapoartelor de analiză. Temeiurile legale uzuale includ, după caz:

- executarea unui contract sau demersuri la cererea persoanei vizate (art. 6 alin. (1) lit. b)
- îndeplinirea unei obligații legale (art. 6 alin. (1) lit. c) – de ex. arhivare, raportări, cerințe sanitare/financiare

- interes public / exercitarea autorității publice, când este aplicabil (art. 6 alin. (1) lit. e)
- interese legitime (art. 6 alin. (1) lit. f) – de ex. securitate, prevenirea fraudei, apărarea drepturilor în justiție, cu evaluare LIA

Pentru categoriile speciale de date (date privind sănătatea, date genetice), prelucrarea se realizează în principal în temeiul art. 9 alin. (2) lit. h) (medicină preventivă, diagnostic medical, furnizarea de îngrijiri sau tratamente) și/sau alt temei aplicabil, cu respectarea secretului profesional.
Consimțământul este utilizat atunci când este necesar (de ex. comunicări de marketing/informări opționale), putând fi retras oricând, fără a afecta legalitatea prelucrării anterioare retragerii.

Categorii de date prelucrate (exemple)

- date de identificare și contact: nume, CNP/serie act (dacă este necesar), adresă, telefon, e-mail, date aparținători (unde e cazul)
- date medicale și genetice: indicație, diagnostic/suspiciune, rezultate analize, date probă, imagini/histopatologie (dacă este cazul)
- date administrative/financiare: facturi, plăți, decontări, date contractuale
- date tehnice și de securitate: loguri de acces, audit trail în LIS/IT, evidențe de trasabilitate probă-rezultat
- date personal/HR (pentru angajați/colaboratori): date contractuale, pontaj, instruiri, evaluări, după caz

Acces, confidențialitate și securitatea datelor

Laboratorul aplică principiul „need-to-know”, accesul la date fiind acordat pe roluri și responsabilități, cu autentificare, parole/MFA unde este posibil, și jurnalizare (audit trail) pentru sistemele informatice critice.
Personalul are obligația de confidențialitate, inclusiv după încetarea raporturilor de muncă/colaborare.
Măsurile tehnice și organizatorice includ, după caz:

- control acces fizic și logic; segregare roluri; politici de parole; blocare automată; revizuire periodică a drepturilor
- backup, restaurare și plan de continuitate; testarea periodică a copiilor de siguranță
- protecție împotriva malware; actualizări de securitate; management vulnerabilități
- transmiterea rezultatelor prin canale controlate; criptare/anonimizare/pseudonimizare, unde este fezabil
- protecția documentelor pe hârtie: depozitare securizată, arhivare, acces controlat, distrugere securizată
- controale de integritate a datelor și trasabilitate probă-rezultat, în acord cu cerințele SR EN ISO 15189:2023

Destinatari, persoane împuternicite și transferuri

Datele pot fi comunicate numai către destinatari autorizați și în măsura necesară: persoane vizate, medici trimițători, unități sanitare/parteneri contractuali, autorități publice competente, asigurători/decontatori (unde este aplicabil), precum și către persoane împuternicite (ex. furnizori IT, curierat, arhivare, mentenanță), în baza unor contracte care includ clauze de confidențialitate și acorduri de împuternicire (DPA), cu cerințe de securitate.
Transferurile către state terțe/organizații internaționale, dacă sunt necesare, se realizează numai cu garanții adecvate (de ex. decizie de adecvare, clauze contractuale standard) și cu evaluarea riscurilor aplicabile.

Perioade de păstrare și arhivare

Perioadele de păstrare sunt stabilite conform legislației aplicabile, obligațiilor profesionale și contractuale, precum și cerințelor privind păstrarea înregistrărilor din SR EN ISO 15189:2023. După expirarea termenelor, datele se elimină/distrug securizat sau se anonimizează, după caz.

Drepturile persoanelor vizate și modul de exercitare

Persoanele vizate pot exercita drepturile prevăzute de GDPR (acces, rectificare, restricționare, opoziție, portabilitate, ștergere în măsura aplicabilă, retragerea consimțământului). Solicitările se transmit laboratorului prin canalele de contact comunicate în informarea pacientului/pe site. Laboratorul răspunde în termenele GDPR și poate solicita informații rezonabile pentru verificarea identității.

Anumite drepturi pot fi limitate atunci când există obligații legale de păstrare a datelor, cerințe de sănătate publică ori necesitatea apărării drepturilor și intereselor legitime ale laboratorului, cu respectarea cadrului legal.

Gestionarea incidentelor și a încălcărilor de securitate

Orice incident/suspiciune privind securitatea datelor se raportează imediat către management și/sau responsabilul desemnat. Laboratorul investighează incidentul, aplică măsuri de limitare și remediere și documentează evenimentul. Dacă este incident de tip „data breach” care poate genera risc pentru drepturile și libertățile persoanelor vizate, se evaluează necesitatea notificării autorității de supraveghere în termen de 72 de ore și, după caz, a informării persoanelor vizate.

Comunicare și informare

Laboratorul pune la dispoziția persoanelor vizate o informare GDPR (notă de informare) în punctele de contact relevante (recoltare/recepție/online) și, după caz, în contracte și materiale informative, astfel încât să fie clar: cine prelucrează datele, în ce scop, pe ce temei, categoriile de date, destinatarii, perioadele de stocare și drepturile persoanelor vizate.

Aprobat

Data: 31.12.2025

Manager: Fazakas Zoltán-József