Politică de confidențialitate
pentru datele cu caracter personal a clienților IPAD ”PAYNET”, colectate în cadrul procesului de identificare la distanță eKYC și date biometrice

/versiune actualizată la 21.10.2026/

Politica de confidențialitate aferentă soluției și procesului pentru identificarea la distanță (eKYC) pentru clienții IPAD «Paynet»” și utilizarea datelor biometrice

1. Această politică descrie modul în care „Paynet Services” S.R.L. (în continuare „Paynet”) prelucrează datele tale cu caracter personal ale clienților persoane fizice, inclusiv datele biometrice (imaginea feței), atunci când folosești procesul de identificare la distanță (electronic Know Your Customer – eKYC) pentru deschiderea și utilizarea Instrumentului de Plată cu Acces la Distanță (IPAD) „Paynet” și a serviciilor conexe. Ea este elaborată în conformitate cu legislația națională privind protecția datelor cu caracter personal, legislația privind prevenirea spălării banilor și finanțării terorismului, precum și cu actele normative și regulamentele relevante ale Băncii Naționale a Moldovei (BNM).
Pentru alte prelucrări de date (de exemplu, executarea plăților, programe de loialitate, marketing, relații cu furnizori, resurse umane, utilizarea website-ului sau a altor servicii Paynet) se aplică Regulamentul general privind prelucrarea datelor cu caracter personal al Paynet, disponibil în compartimentul ”Termeni și condiții” din aplicația ”Paynet Portofel” și pe pagina-web: www.paynet.md.
Această politică completează Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul Paynet (inclusive Politica privind retenția, ștergerea și anonimizarea datelor cu caracter personal a ”Paynet Services” S.R.L.). În cazul în care există diferențe, pentru procesul eKYC se aplică dispozițiile prezentei politici, fără a afecta obligațiile legale și de reglementare aplicabile.

2. Cine suntem și cum ne poți contacta
Operatorul de date este „Paynet Services” S.R.L. (IDNO: 1013600036596), în calitate de prestator al IPAD „Paynet”. Pentru întrebări legate de protecția datelor personale ne poți contacta la adresa de E-mail: privacy@paynet.md.

3. Ce date prelucrăm în procesul eKYC
În cadrul identificării la distanță prelucrăm, în principal, următoarele categorii de date:

a) Date de identificare și contact
   - nume, prenume;
   - cod personal (IDNP);
   - data nașterii, cetățenie;
   - adresa de domiciliu/reședință;
   - date din documentul de identitate (serie, număr, emitent, data expirării);
   - date de contact (telefon, e-mail).

b) Date din documentul de identitate
   - imaginea documentului (față/verso);
   - date citite automat (OCR) din zona tipărită și/sau zona de citire automată (MRZ);
   - rezultatele verificărilor de valabilitate și autenticitate a documentului, inclusiv răspunsuri primite de la autorități sau sisteme externe (de exemplu, ASP/MConnect) în măsura permisă de lege.

c) Date biometrice (recunoaștere facială)
   - fotografia feței tale realizată în aplicație;

- scurte secvențe video și/sau mai multe cadre folosite pentru a verifica faptul că ești o persoană reală (verificare anti-fraudă);
- rezultatele tehnice ale comparației dintre fotografia ta și fotografia din documentul de identitate (de exemplu, scorul de potrivire și rezultatul verificării, indicatori tehnici aferenți procesului de recunoaștere facială);
- În cursul fluxului tehnic pot fi generate temporar și date biometrice brute (de exemplu, secvențe video complete, cadre multiple „raw"); aceste date sunt păstrate numai pe o perioadă limitată, strict necesară pentru funcționarea fluxului, rezolvarea incidentelor tehnice și investigarea tentativelor de fraudă, după care sunt șterse în condițiile Politicii de retenție.

d) Date KYC/AML
   - răspunsuri din chestionarul „cunoașterea clientelei" [KYC] (scopul relației de afaceri, sursa fondurilor, profil tranzacțional estimat, beneficiarul efectiv (dacă este cazul), statut de persoană expusă politic [PEP] etc.);
   - rezultatele verificărilor pe liste de sancțiuni și persoane expuse politic (PEP);
   - scoruri de risc și decizii KYC/AML, inclusiv justificări interne (note, comentarii) privind acceptarea sau refuzul clientului sau impunerea unor măsuri suplimentare.

e) Date tehnice și de securitate
   - informații despre dispozitiv și aplicație (de exemplu, tip/model dispozitiv, sistem de operare, versiune aplicație),), în măsura în care acestea sunt necesare pentru protejarea sistemului și prevenirea fraudelor;
   - adresa IP, informații despre conexiune, data și ora acțiunilor în aplicație, coduri de eroare;
   - loguri care arată pașii parcurși în procesul de identificare, acceptarea informațiilor și a termenilor, autentificări și autorizări, loguri privind executarea operațiunilor de plată și a altor acțiuni relevante.

f) Date tranzacționale și operaționale IPAD
   - date despre tranzacțiile efectuate prin IPAD „Paynet" (sume, conturi, IBAN, beneficiari, data/ora, canal, referințe etc.);
   - istoricul operațiunilor relevante pentru monitorizarea tranzacțiilor și îndeplinirea obligațiilor AML/CFT, contabilitate și raportare.

Actualizarea periodică a datelor KYC (fără re-selfie inutil)

Pe lângă identificarea inițială prin eKYC, Paynet are obligația legală să își actualizeze periodic datele despre clienți (KYC – „Know Your Customer").

Pentru clienții existenți:

- Folosim IDNP-ul și datele deja înregistrate pentru a verifica automat, prin ASP (prin intermediul MConnect), dacă documentul tău de identitate este încă valabil și este același.
- Dacă ASP confirmă că documentul este același și nu au apărut modificări relevante:
  - NU îți mai cerem din nou fotografii ale documentului și selfie / video liveness;
  - îți vom cere doar să confirmi sau să actualizezi informațiile din chestionarul KYC (de exemplu: sursa veniturilor, volumul estimat al tranzacțiilor, scopul relației de afaceri).
- Doar dacă ASP ne indică faptul că ai un document nou (de exemplu, ai schimbat buletinul), îți vom cere să parcurgi din nou fluxul complet eKYC, inclusiv fotografierea noului document și selfie / video pentru liveness.

Acest mod de lucru ne ajută:

- să respectăm cerințele legale AML/KYC privind actualizarea datelor;
- să reducem numărul de situații în care îți cerem din nou date biometrice (selfie/video);

- să evităm colectarea și stocarea inutilă de imagini și filmări cu tine.

4.De unde obținem datele

În principal, datele sunt obținute direct de la tine, atunci când:

- vă creați contul și parcurgeți fluxul de identificare la distanță prin aplicația mobilă sau platforma IPAD „Paynet";
- încărcați sau prezentați documentele de identitate;
- completați chestionarul KYC sau alte formulare electronice.

În plus, în măsura permisă de lege, putem obține și verifica anumite date din surse externe, cum ar fi:

- sisteme și platforme oficiale (de exemplu, ASP/MConnect) – pentru confirmarea identității și verificarea documentelor;
- liste de sancțiuni și PEP, baze de date utilizate în scopuri AML/CFT;
- instituții financiare și alte entități implicate în executarea tranzacțiilor.

5. De ce prelucrăm aceste date (scopuri)

Prelucrăm datele tale în procesul eKYC, inclusiv datele biometrice, pentru:

a) Verificarea identității la distanță (eKYC) și deschiderea contului de plăți
   - confirmarea faptului că tu ești titularul documentului de identitate prezentat
   - îndeplinirea cerințelor de identificare a clientului prin mijloace electronice, conform reglementărilor BNM;
   - verificarea autenticității documentului;
   - documentarea rezultatului procesului de identificare;
   - deschiderea și administrarea contului de plăți prin IPAD „Paynet".

b) Îndeplinirea obligațiilor legale de „cunoaștere a clientelei" (Know Your Customer – KYC) și prevenire a spălării banilor și finanțării terorismului (Anti-Money Laundering / Combating the Financing of Terrorism – AML/CFT)
   - respectarea cerințelor din Legea nr. 308/2017 privind prevenirea și combaterea spălării banilor și finanțării terorismului și a reglementărilor Băncii Naționale a Moldovei (BNM);
   - efectuarea de verificări în baza de date și pe liste de sancțiuni;
   - monitorizarea tranzacțiilor și detectarea tranzacțiilor suspecte;
   - păstrarea dovezilor de identificare pentru perioada prevăzută de lege;
   - raportarea către autoritățile competente (de exemplu, Serviciul Prevenirea și Combaterea Spălării Banilor), atunci când legea ne obligă.

c) Securitatea sistemului și prevenirea fraudei
   - Prevenirea, detectarea și investigarea accesului neautorizat la contul tău;
   - detectarea și investigarea tentativelor de fraudă sau abuz;
   - asigurarea integrității și continuității sistemului nostru de plăți;
   - audit intern și extern, verificări tehnice și de conformitate.

d) Respectarea obligațiilor noastre contractuale față de tine
   - furnizarea serviciilor de plată și funcționarea IPAD „Paynet";
   - contactarea ta atunci când este necesar pentru utilizarea serviciului (informații despre sold, tranzacții, notificări legate de cont și servicii).

e) Îndeplinirea obligațiilor legale și de reglementare
   - păstrarea evidențelor și documentelor justificative pentru termenele prevăzute de legislația AML/CFT, de reglementările BNM și de legislația fiscală/contabilă;
   - răspunsul la solicitările autorităților (de exemplu, BNM, CNPDCP, organe de anchetă) în limitele legii.

f) Gestionarea reclamațiilor și a drepturilor persoanelor vizate

- soluționarea solicitărilor, reclamațiilor și reclamațiilor legate de serviciile Paynet sau de prelucrarea datelor;
- documentarea și dovedirea conformității noastre față de legislația privind protecția datelor.

g) Marketing și comunicări comerciale (doar dacă este cazul și distinct de eKYC)
   - Pentru comunicări de marketing direct (newsletter, oferte, informații comerciale), folosim datele tale doar dacă avem un temei corespunzător (de exemplu, consimțământul, acolo unde este cerut de lege). Aceste prelucrări sunt separate de fluxul de eKYC și le vom explica în mod distinct, în politicile și informările aferente marketingului.

Nu folosim datele tale biometrice pentru scopuri de marketing, publicitate și nu vindem datele tale unor terți.

6. Care este temeiul juridic al prelucrării

Prelucrarea datelor tale în procesul eKYC, inclusiv a datelor biometrice, se bazează în principal pe:

- obligații legale ale Paynet de a te identifica și de a aplica măsurile de prevenire și combatere a spălării banilor și finanțării terorismului (Legea nr. 308/2017 și reglementările BNM);
- executarea contractului sau demersurile pentru încheierea contractului privind IPAD „Paynet" și serviciile de plată aferente (de exemplu, deschiderea IPAD, furnizarea serviciilor de plată);
- un interes public important legat de integritatea sistemului financiar și de prevenirea spălării banilor și finanțării terorismului și a fraudei, în măsura permisă de legislația aplicabilă;
- interesul legitim al Paynet de a asigura securitatea sistemelor și a conturilor de plăți, prevenirea fraudelor și apărarea drepturilor noastre în caz de litigii.

Consimțământul tău, exprimat prin continuarea procesului de identificare la distanță, are rolul de a confirma că ai înțeles cum sunt prelucrate datele tale și că alegi acest canal de identificare, dar nu este temeiul juridic principal al prelucrării datelor biometrice în scop KYC/AML. Regulamentul BNM privind identificarea prin mijloace electronice prevede că, înainte de utilizarea acestor mijloace, clientul trebuie să fie informat și să-și exprime acordul pentru utilizarea canalului electronic. În acest context acordul exprimat în aplicație este tratat ca acord procedural privind utilizarea canalului eKYC; el nu schimbă temeiul juridic principal pentru prelucrarea datelor (obligație legală, contract, interes public/legitim) și nu creează iluzia că prelucrarea datelor KYC/AML poate fi oprită oricând prin retragerea consimțământului, câtă vreme legea ne obligă să păstrăm anumite date pe o perioadă minimă.

Pentru activități care nu sunt strict legate de KYC/AML/securitate (de exemplu, marketing), putem utiliza, acolo unde este necesar, consimțământul tău liber exprimat, colectat și gestionat separat de fluxul eKYC și cu informare distinctă.

7. Cât timp păstrăm datele

- Dosarul de identificare și datele KYC/AML (inclusiv imaginea „best shot" a feței și rezultatele verificărilor biometrice) se păstrează pe durata relației tale de afaceri cu Paynet + cel puțin 5 ani după încetare, conform Legii nr. 308/2017 și reglementărilor BNM.
- Datele biometrice „brute" (de exemplu, cadre video multiple sau imagini intermediare care nu sunt folosite ca probă finală) se păstrează pe o perioadă scurtă, limitată la maximum 90 de zile de la finalizarea procesului, doar pentru a rezolva incidente tehnice și a investiga fraude, după care sunt șterse automat sau anonimizate ireversibil, cu excepția cazului în care legea cere altfel (de exemplu, în caz de litigii sau investigații oficiale).
- Logurile tehnice și de securitate se păstrează, în general, între 12 și 24 de luni, iar unele loguri critice pot fi păstrate mai mult, atunci când este necesar pentru securitate sau pentru respectarea cerințelor de reglementare.

Detaliile privind termenele de retenție sunt prevăzute în Politica Paynet privind retenția, ștergerea și anonimizarea datelor, care este pusă la dispoziția autorităților și poate fi consultată la cerere în condițiile legii.

Această politică de confidențialitate și Politica de retenție trebuie citite împreună și sunt aliniate cu Evaluarea de impact asupra protecției datelor (DPIA) pentru soluția eKYC.

8. Cui putem transmite datele tale

În funcție de situație, datele tale pot fi transmise:

- autorităților competente, atunci când legea ne obligă (de exemplu BNM, Serviciul Prevenirea și Combaterea Spălării Banilor, organe de urmărire penală, instanțe de judecată);
- furnizorilor de servicii tehnice, care ne ajută să implementăm identificarea la distanță (de exemplu, furnizori ai modulului de recunoaștere facială și verificare a documentelor), în calitate de persoane împuternicite de operator, în baza unor contracte care includ clauze ferme de protecție a datelor. Acești furnizori nu au voie să folosească datele tale în scopuri proprii și nu le pot transmite mai departe fără acordul și instrucțiunile noastre, cu excepția cazurilor prevăzute de lege;
- platforme și servicii de interconectare cu registre oficiale (de exemplu, ASP/MConnect), în măsura în care acest lucru este permis de lege și strict necesar pentru verificarea identității și a documentelor;
- auditori, consultanți sau alți specialiști externi (de exemplu, consultanți în domeniul protecției datelor, experți IT/ale securității), în măsura necesară pentru audit, conformitate și gestionarea riscurilor, cu garanții contractuale adecvate;
- altor instituții financiare sau parteneri, în măsura în care acest lucru este prevăzut de lege sau de contract și este necesar pentru efectuarea unor operațiuni de plată ori pentru prevenirea fraudei.

Nu vindem datele tale unor terți pentru marketing și nu permitem utilizarea datelor biometrice în alte scopuri decât cele descrise în această politică.

9. Transferuri de date în afara Republicii Moldova

În mod obișnuit, Paynet urmărește ca datele să fie stocate și prelucrate în infrastructuri aflate în Republica Moldova sau în state care asigură un nivel adecvat de protecție.

Dacă, în mod excepțional, este necesar transferul unor date către furnizori sau servere situate în alte state, Paynet se asigură că există un temei juridic corespunzător pentru transfer; sunt aplicate garanții adecvate de protecție (de exemplu, clauze contractuale, măsuri tehnice și organizatorice suplimentare); persoanele vizate sunt informate în mod corespunzător, atunci când legislația impune acest lucru.

10. Drepturile tale

În condițiile legii aplicabile, ai următoarele drepturi cu privire la datele tale personale:

- dreptul de acces (să știi ce date prelucrăm despre tine);
- dreptul la rectificare (corectarea datelor inexacte sau incomplete);
- dreptul la restricționarea prelucrării, în anumite situații;
- dreptul la opoziție, în cazurile prevăzute de lege;
- dreptul la portabilitatea datelor, în măsura în care este aplicabil;
- dreptul la ștergerea datelor („dreptul de a fi uitat”), în măsura în care nu există obligații legale de păstrare (în special în domeniul AML/KYC);
- dreptul de a depune o plângere la autoritatea de supraveghere (Centrul Național pentru Protecția Datelor cu Caracter Personal - CNPDCP) dacă consideri că drepturile tale au fost încălcate.

În unele cazuri, nu putem șterge anumite date (de exemplu, datele din dosarul KYC/AML și anumite loguri), deoarece legea ne obligă să le păstrăm o perioadă minimă (în general, cel puțin 5 ani după încetarea relației de afaceri) sau datele sunt necesare pentru apărarea unui drept în instanță, pentru investigarea fraudelor sau pentru alte proceduri oficiale..

Pentru a-ți exercita drepturile, ne poți contacta folosind datele de contact de la secțiunea „Cine suntem și cum ne poți contacta”. Vom răspunde, de regulă, în termen de 30 de zile calendaristice, cu respectarea prevederilor legale.

11. Cum protejăm datele tale

Paynet aplică măsuri tehnice și organizatorice adecvate pentru a asigura confidențialitatea, integritatea și disponibilitatea datelor, inclusiv:

- control strict al accesului la date, pe baza rolurilor și a principiului „need-to-know”;
- criptarea datelor și a canalelor de comunicație, acolo unde este necesar;
- jurnalizarea și monitorizarea accesului și a operațiunilor relevante;
- politici de backup și recuperare în caz de dezastru;
- proceduri de ștergere și distrugere sigură a datelor și mediilor de stocare, după expirarea termenelor de retenție;
- audit și testări periodice ale sistemelor, inclusiv în ceea ce privește soluțiile biometrice utilizate.

12. Ce se întâmplă dacă nu dorești să folosești identificarea la distanță

Dacă nu dorești să utilizezi identificarea la distanță prin biometrie facială, te rugăm să ne contactezi pentru a afla dacă există alte canale alternative de identificare (de exemplu, la un punct fizic sau prin alte mijloace permise de legislație și de reglementările BNM).

Dacă, la momentul respectiv, Paynet pune la dispoziție un canal alternativ de identificare, îți vom comunica aceste opțiuni. În lipsa unui astfel de canal alternativ, identificarea la distanță poate fi singura modalitate disponibilă pentru deschiderea contului.

13. Actualizări ale acestei politici

Putem actualiza periodic prezenta Politică de confidențialitate pentru:

- a reflecta modificări ale cadrului legal sau de reglementare;
- a integra schimbări în arhitectura tehnică sau în fluxurile de prelucrare (de exemplu, extinderea funcționalităților eKYC, utilizarea unor noi furnizori sau module software);
- a clarifica sau detalia anumite aspecte, în funcție de recomandările autorităților sau de bunele practici.

Versiunea actualizată va fi disponibilă în aplicația și pe site-ul Paynet (de exemplu, prin linkul afișat în cadrul procesului de identificare la distanță). Vom indica întotdeauna data ultimei actualizări.