Anexa B — Acord de prelucrare a datelor (DPA)

Versiunea KIV-1.11 · din 12 noiembrie 2026.

Acordul devine parte a contractului când Clientul acceptă Termenii, prin bifa de la crearea contului. Anexa B-P este formată din datele firmei din Companie și configurația publicată a cardului. Ele se păstrează înainte ca primul client să se înscrie; publicarea documentului nu ține loc de acceptare.

B1. Părți, roluri și obiect

Clientul, afacerea care și-a deschis contul pe mereu.md, identificată prin datele firmei din Companie, este „Operatorul” pentru programul său de fidelitate. KIV MINDS S.R.L., CUI 47345847, sediul România, județul Iași, municipiul Iași, str. Stihii nr. 2A, et. 6, ap. 16, cod poștal 700083, contact@mereu.md, este „Persoana împuternicită” pentru operațiunile executate în numele Operatorului.

Acest acord reglementează prelucrarea de către KIV MINDS, stabilită în România, potrivit GDPR și legislației române aplicabile. Pentru operațiunile aflate și în domeniul Legii Republicii Moldova nr. 195/2024 se respectă suplimentar normele imperative aplicabile. Limitarea comercială la afaceri din Moldova nu înlătură obligațiile GDPR ale KIV MINDS. Acordul nu reglementează ca împuternicire prelucrările proprii Mereu de facturare, administrare a relației contractuale sau celelalte scopuri proprii explicate în politica de confidențialitate.

Dacă Operatorul acționează, la rândul său, ca persoană împuternicită a altuia, el identifică operatorul inițial și dovedește autorizarea lanțului înainte de activare. Orice scop comun sau propriu nou necesită clarificarea rolurilor înainte de prelucrare. Rolurile nu pot fi stabilite contrar activității reale.

B2. Instrucțiuni și obligațiile Operatorului

Mereu prelucrează numai pe baza instrucțiunilor documentate ale Operatorului, inclusiv pentru transferuri internaționale, exceptând o obligație legală aplicabilă Mereu. În acest ultim caz informează Operatorul înainte de prelucrare, dacă legea nu interzice. Contractul, anexele și comenzile utilizatorilor autorizați constituie instrucțiuni numai în limitele funcțiilor și scopurilor aprobate.

Mereu informează imediat Operatorul dacă apreciază că o instrucțiune încalcă legislația datelor și suspendă operațiunea afectată până la clarificare; nu execută o instrucțiune vădit ilegală. Schimbările materiale de scop, categorie de date, destinatari sau durată se documentează înainte de aplicare.

Operatorul răspunde pentru temeiurile legale, informarea persoanelor, exactitatea și minimizarea datelor, legalitatea importurilor, regulile programului și instrucțiunile sale. El nu colectează date sensibile ori date ale minorilor printr-o configurație obișnuită fără analiza și măsurile specifice necesare. Mereu rămâne responsabil pentru propriile obligații legale și contractuale; garanțiile Operatorului nu îl exonerează.

B3. Confidențialitate și limite de utilizare

Accesul este permis numai persoanelor autorizate, în limita necesității, supuse unor obligații de confidențialitate legale sau contractuale. Mereu instruiește personalul relevant și retrage accesul la încetarea atribuțiilor.

Mereu nu vinde datele, nu creează profiluri comune între afaceri și nu le folosește pentru publicitatea proprie sau antrenarea modelelor AI. Pseudonimizarea nu transformă automat datele în date anonime. Statistici proprii pot fi folosite în afara instrucțiunilor numai dacă sunt efectiv anonime, fără posibilitate rezonabilă de reidentificare; simpla etichetare ca „agregat” nu este suficientă.

B4. Măsuri tehnice și organizatorice

Mereu implementează măsuri proporționale cu riscul, conform articolului 32 GDPR și celorlalte norme aplicabile, incluzând:

- izolarea logică a organizațiilor și verificarea drepturilor la fiecare acces relevant;
- acces minim necesar, protecția autentificării, administrarea privilegiilor, revocarea accesului și evidențe de administrare;
- criptarea transportului, protejarea bazelor, fișierelor și copiilor de siguranță potrivit clasificării lor; păstrarea separată și acces controlat la chei;
- hash securizat al parolelor, protejarea tokenurilor și certificatelor Wallet, rotație și procedură pentru compromitere;

- actualizări de securitate, gestionarea vulnerabilităților, limitarea abuzurilor și dezvoltare cu verificări proporționale;
- minimizarea jurnalelor și excluderea parolelor, cheilor private, CVV și datelor personale inutile;
- copii de siguranță cu acces restrâns și reaplicarea ștergerilor înainte de revenirea datelor în utilizare; pentru configurația curentă nu este confirmat un termen maxim automat de expirare a tuturor copiilor, inclusiv a copiilor de dinaintea actualizărilor;
- proceduri pentru incidente, acces, rectificare, restricționare, export și ștergere, cu verificarea identității proporțională;
- verificarea periodică a eficacității măsurilor și remedierea deficiențelor.

Anexa B-S descrie măsurile efectiv disponibile, limitele și verificările. Nu se afirmă existența unei certificări ISO/SOC, a criptării integrale sau a unei funcții neimplementate. Măsurile pot evolua fără reducerea protecției convenite. Un risc care împiedică garantarea măsurilor necesare se comunică și blochează prelucrarea afectată până la remediere.

B5. Subcontractanți

Operatorul acordă autorizare generală numai pentru subcontractanții **identificați în registrul anexat și acceptat**, cu serviciu, entitate juridică, țări, categorii de date și garanții. Un rând necompletat nu constituie autorizare. Mereu impune prin contract obligații de protecție cel puțin echivalente pentru operațiunile delegate și răspunde față de Operator pentru îndeplinirea lor potrivit legii.

Mereu notifică în prealabil adăugarea ori înlocuirea unui subcontractant, cu cel puțin 30 de zile calendaristice înainte de acces, și oferă informațiile necesare evaluării. Operatorul poate formula obiecții motivate de protecția datelor în acest interval. Părțile caută o soluție; dacă nu există una adecvată, operațiunea afectată nu se încredințează noului furnizor, iar serviciul afectat poate înceta fără penalitate, cu regularizarea prestațiilor neexecutate.

Pentru o urgență reală de securitate se aplică măsuri de continuitate și notificare fără întârziere; urgența nu înlocuiește autorizarea legal necesară. Apple, Google și băncile nu sunt etichetați automat subcontractanți pentru toate activitățile lor. Rolul

se stabilește pentru fiecare serviciu și scop. Divulgarea către un operator independent trebuie să aibă instrucțiune, temei și informare proprii.

B6. Transferuri internaționale

Găzduirea este în Germania, iar administrarea se face din Republica Moldova. Furnizorii de comunicații și Wallet pot prelucra date în alte țări, conform registrului și funcțiilor folosite.

Înaintea transferului, Mereu documentează destinatarii, țările și mecanismul legal cerut de Legea nr. 195/2024: un nivel de protecție recunoscut sau garanții adecvate, după caz. Când GDPR este aplicabil operațiunii, se respectă și cerințele sale privind transferurile. Clauzele standard se încheie în forma aplicabilă, cu părțile și anexele completate; un link nu ține loc de acord.

Acceptarea Termenilor nu este consimțământ general pentru transferuri fără garanții. Mereu pune la dispoziție informațiile relevante și, dacă garanțiile nu mai pot fi respectate, informează Operatorul și remediază ori suspendă transferul afectat.

B7. Drepturile persoanelor și asistență

Mereu transmite Operatorului cererile privind programul fără întârziere nejustificată, ca angajament contractual în cel mult două zile lucrătoare de la identificarea lor, și nu răspunde în numele Operatorului fără instrucțiuni, exceptând obligațiile legale. Cererile privind scopurile proprii Mereu sunt tratate direct de Mereu.

Ținând seama de natura prelucrării, Mereu acordă asistență tehnică și organizatorică pentru informare, acces, rectificare, ștergere, restricționare, portabilitate, opoziție, retragerea consimțământului și verificarea deciziilor automate. Datele se transmit securizat persoanei autorizate. Lipsa unei funcții automate nu justifică refuzul unei cereri care poate fi executată asistat.

Mereu oferă informațiile disponibile necesare evaluărilor de impact, consultării prealabile, securității și notificărilor legale, potrivit legislației aplicabile. Asistența obișnuită pentru obligațiile sale este inclusă în serviciu. Orice cost pentru asistență extraordinară trebuie să fie proporțional, convenit anticipat și să nu împiedice exercitarea unui drept sau îndeplinirea unei obligații imperative.

B8. Incidente

Mereu notifică Operatorul fără întârziere nejustificată după ce ia cunoștință de o încălcare a securității datelor prelucrate în numele acestuia. Părțile stabilesc suplimentar un termen contractual de cel mult **24 de ore pentru notificarea inițială**, care nu permite amânarea nejustificată până la expirarea lui. Nu se așteaptă finalizarea investigației.

Informarea inițială și completările succesive includ natura incidentului, categoriile și numărul aproximativ de persoane/înregistrări cunoscute, consecințele probabile, măsurile luate sau propuse, contactul responsabil și limitele informațiilor disponibile. Mereu limitează incidentul, păstrează probele necesare și cooperează la remediere.

Operatorul decide notificarea autorității și persoanelor pentru prelucrările sale, fără a exclude obligații directe ale Mereu. Termenul legal de 72 de ore pentru notificarea autorității, când este aplicabil, nu este termenul pe care Mereu îl poate consuma înainte să informeze Operatorul. Mereu nu face declarații în numele Operatorului fără mandat, exceptând obligația legală.

B9. Evidențe și audit

Mereu păstrează evidențele cerute de lege și pune la dispoziție informațiile necesare dovedirii respectării acordului. Permite și contribuie la audituri și inspecții ale Operatorului sau auditorului mandatat, cu protejarea datelor altor clienți și a secretelor de securitate.

În mod obișnuit se folosesc mai întâi documentele și verificările la distanță, apoi o inspecție proporțională, anunțată rezonabil. Frecvența ori preavizul uzual nu limitează auditul justificat de un incident, o suspiciune serioasă sau cererea autorității. Nu se percep tarife prohibitive și nu se impune renunțarea la audit. Deficiențele se remediază într-un calendar justificat de risc.

B10. Returnare și ștergere

La alegerea Operatorului, Mereu returnează datele prin export securizat și apoi le șterge sau le șterge direct, inclusiv copiile, dacă o obligație legală nu impune

păstrarea. Exportul acoperă categoriile din anexa B-P, inclusiv evidențele relevante ale acordurilor, nu doar datele vizibile pe card.

Termenele și criteriile de păstrare disponibile sunt cele descrise în prezentul acord și în Politica de confidențialitate. Configurația din cabinet nu este o anexă completată cu termene de expirare pentru toate fișierele, jurnalele, mesajele și copiile de siguranță. Pentru configurația curentă nu este confirmat un termen maxim automat de expirare a tuturor copiilor. Cererile se tratează asistat, prin inventarierea și eliminarea copiilor relevante ori documentarea obligației concrete de păstrare. Un ciclu de backup nu amână ștergerea din sistemul activ.

Datele din copiile reziduale se izolează și nu trebuie readuse în utilizare la restaurare fără reaplicarea ștergerilor. Păstrarea obligatorie se documentează prin temei, categorii, termen și acces limitat. Mereu confirmă finalizarea numai după verificarea rezultatului și indică transparent reziduurile, copiile încă neeliminate ori operațiunile în curs la un furnizor. Nu numește „ștergere completă” simpla inactivare a unui obiect Google sau revocarea unui link.

Copiile salvate de Participant și prelucrările operatorilor independenți se tratează prin mecanismele lor; Mereu asistă în limitele controlului său. Înregistrările necesare dovedirii ștergerii sunt minimizate și au propriul termen justificat.

B11. Durată și prioritate

Acordul rămâne aplicabil cât timp Mereu ori subcontractanții săi dețin datele acoperite. Modificările se documentează și nu reduc garanțiile retroactiv. Încălcarea esențială poate determina suspendarea prelucrării ori încetarea serviciului afectat potrivit legii. Drepturile persoanelor vizate, autorităților și răspunderea obligatorie nu pot fi limitate prin contract.

B-P. Parametrii programului contractat

Datele firmei și configurația publicată formează anexa individuală. Ele identifică Operatorul și contactul său pentru date (emailul pentru întrebări despre date sau, până îl scrie, emailul contului), programul și locațiile, scopurile, categoriile de persoane, câmpurile efective, volumul estimat, serviciile Wallet, canalele și durata. Modificările se documentează înainte de aplicare.

Operațiunile autorizate sunt colectarea, înregistrarea, organizarea, consultarea, actualizarea, calculul beneficiilor, transmiterea autorizată, exportul, restricționarea și ștergerea, în limitele funcțiilor comandate. Persoanele vizate sunt participanții și reprezentanții/personalul Clientului pentru operațiunile făcute în numele său.

Datele pot include numele afișat, contactele justificate, identificatorii cardului și programului, soldul și operațiunile, inclusiv cumpărăturile înregistrate de personalul Operatorului (data, locația, suma, reducerea, punctele și utilizatorul care le-a înregistrat), acceptările și preferințele, metadatele Wallet necesare și comunicările autorizate. Câmpurile opționale, inclusiv ziua și luna aniversării, cer un scop și o instrucțiune expresă; nu se presupune colectarea anului nașterii. Nu sunt autorizate implicit categorii speciale, biometrie, acte de identitate, condamnări, parole ale furnizorilor ori date complete de card bancar.

Durata prelucrării urmează serviciul, instrucțiunile justificate ale Operatorului și obligațiile legale. Evenimentul de la care curge un termen, durata ori criteriul disponibil și excepțiile sunt cele descrise aici și în Politica de confidențialitate; cabinetul nu generează o evidență completă a termenelor și a ștergerii copiilor. Soldul, activitatea și contestațiile se tratează distinct de simpla vechime a unui card. Cardul intră în curățenia automată după 2 ani fără activitate relevantă: înscriere, cumpărătură sau vizită valabilă, modificare manuală ori programare. După ștergere, cumpărăturile rămân în totalurile Operatorului fără legătură cu cardul. După 90 de zile calendaristice consecutive de oprire pentru neplată, contractul se încheie; anularea reînnoirii Stripe încheie contractul la sfârșitul perioadei achitate. Urmează 90 de zile calendaristice pentru export, apoi ștergerea sau anonimizarea datelor clienților. Facturile și dovezile plăților se păstrează separat potrivit obligațiilor legale. Cererile persoanelor se tratează fără a aștepta aceste termene.

Exportul este furnizat într-un format structurat adecvat categoriilor contractate, precum CSV/JSON, împreună cu fișierele originale unde sunt relevante. Categoriile, termenul de răspuns și canalul securizat se stabilesc și se consemnează la tratarea cererii; nu sunt prezentate drept o anexă deja completată automat. Contactul Mereu pentru instrucțiuni și incidente este contact@mereu.md, +373 68 678 274.

B-F. Furnizori și autorizarea programului

Registrul de mai jos descrie infrastructura și destinatarii serviciului. Nu autorizează automat toate utilizările unui furnizor. Pentru prelucrarea în numele Clientului, anexa acceptată identifică furnizorii efectiv folosiți, serviciul, datele, țările și garanțiile; se aplică B5 și B6.

Furnizor/serviciu	Operațiuni și localizare
netcup GmbH — găzduire	Aplicație, bază de date, fișiere și copii locale pe serverul din Germania; administrare KIV MINDS S.R.L. din Moldova
Plus Five Five, Inc. — Resend	Email tranzacțional în fluxurile activate; adresa, conținutul și metadatele de livrare; stocare declarată în SUA
OpenAI Ireland Ltd. — API	Verificarea automată a mesajelor push înainte de trimitere; numele afacerii, titlul și textul mesajului, așa cum le scrie afacerea, fără alte date ale participanților adăugate de Mereu; prelucrare în SUA
Apple — iCloud Mail	Corespondența contact@mereu.md; serviciu distinct de emiterea Wallet; nu este canal implicit pentru exporturi de participanți
Cloudflare — DNS	Rezoluția domeniului; serviciul DNS nu este prezentat ca proxy pentru traficul aplicației
Apple / Google — Wallet	Datele cardului și actualizările când integrarea este activată; profilul și rolurile se identifică separat pentru fiecare platformă
Banca indicată în factură	Transferul bancar pentru plata serviciului și evidențele aferente; nu primește prin această clauză baza participanților. Plata cu cardul bancar nu este activă; un viitor procesator se comunică înainte de folosire

Contractele de subcontractare și mecanismele de transfer se documentează pentru operațiunea efectivă înainte de delegare. Numele public al furnizorului nu este o declarație că fiecare serviciu sau mecanism de transfer al acestuia a fost contractat.

Detaliile relevante se pun la dispoziția Clientului pentru acceptarea anexei și pentru audit, fără expunerea credențialelor.

Pentru utilizarea API de către KIV MINDS S.R.L., stabilită în România, DPA-ul OpenAI identifică OpenAI Ireland Ltd. drept parte pentru clienții din SEE. Acesta prevede obligațiile de persoană împuternicită și mecanismele pentru transferurile internaționale, inclusiv clauzele contractuale standard atunci când sunt aplicabile. Documentația privind datele API indică lipsa folosirii datelor pentru antrenare în mod implicit și păstrarea implicită a jurnalelor de prevenire a abuzului până la 30 de zile, cu excepțiile documentate de furnizor. Mereu nu prezintă această configurație ca Zero Data Retention sau rezidență exclusiv europeană. Documentarea contului și a condițiilor efectiv aplicabile rămâne parte a registrului operațional al furnizorului.

B-S. Securitate și operare

Măsurile contractuale sunt cele din B4. Infrastructura inspectată folosește HTTPS, hash scrypt cu salt pentru parole, sesiuni de autentificare protejate, acces de serviciu restrâns și copii criptate. Aceste măsuri nu sunt prezentate ca certificare de conformitate sau ca garanție că orice integrare viitoare este deja verificată.

Afacerile pornesc singure sau asistat. Colectarea participanților și actualizările Wallet sunt disponibile programelor publicate, în limitele configurației, compatibilității și aprobărilor furnizorilor. Operațiunile de export și ștergere pot necesita asistență. Existența unei copii pe serverul primar nu reprezintă singură recuperare verificată la pierderea completă a serverului.

Înainte de activarea unui program se individualizează instrucțiunile și retenția, se verifică furnizorii și transferurile și se asigură executarea măsurilor necesare. O funcție indisponibilă nu se declară activă prin acceptarea DPA. Mereu informează Clientul despre limite relevante și nu începe operațiunea pe care nu o poate executa în condițiile convenite.

Acceptare: Clientul acceptă acordul prin bifa distinctă pentru KIV MINDS, înainte de plata cu cardul. Păstrăm contul care a bifat, emailul din acel moment, data și ora și versiunea acordului. Datele firmei și configurația publicată se adaugă la salvare. Emailul trebuie confirmat înainte de prima publicare. Cine creează contul declară că are dreptul să reprezinte afacerea (Termeni, §2). KIV MINDS S.R.L. acceptă prin

reprezentantul său autorizat. Nu se acceptă în numele Clientului fără drept de reprezentare.