

TERMENII ȘI CONDIȚIILE DE UTILIZARE A SISTEMULUI INFORMAȚIONAL CU ACCES LA DISTANȚĂ MYIUTE

I. SISTEMUL INFORMAȚIONAL CU ACCES LA DISTANȚĂ MYIUTE ȘI ACCEPTAREA UTILIZĂRII SISTEMULUI:

1. Sistemul informațional cu acces la distanță MyIute este pus la dispoziție de O.C.N. „IuteCredit” S.R.L. (denumită în continuare „**IuteCredit**” sau „**Compania**”), cu sediul în mun. Chișinău, bd. Ștefan cel Mare și Sfânt 182, etajul 5.

2. Termenii și condițiile de utilizare a sistemului informațional cu acces la distanță MyIute (denumiți în continuare „**Termenii MyIute**”), astfel cum sunt stabiliți în prezentul document, sunt și vor fi guvernați și interpretați în conformitate cu legislația Republicii Moldova. **Prin accesarea, utilizarea sau înregistrarea în vederea beneficierii de Sistemul MyIute, acceptați și sunteți de acord să vă asumați caracterul obligatoriu al prezențelor Termenii MyIute.**

3. Prezenții Termenii MyIute constituie acordul juridic dintre Companie și Utilizator, care reglementează accesul la Sistemul MyIute și utilizarea **Sistemului MyIute**. Crearea unui profil MyIute, depunerea unei cereri de produs, finalizarea onboardingului clientului și stabilirea unei relații contractuale constituie etape distincte. Crearea unui profil sau păstrarea unei cereri în formă de proiect nu înseamnă, prin ea însăși, că au fost finalizate măsurile de precauție privind clientul, că a fost stabilită o relație de afaceri sau că Compania a aprobat ori a acordat vreun produs.

4. Vă recomandăm să citiți integral prezenții Termenii MyIute înainte de a decide dacă îi acceptați și dacă doriți să continuați procesul de înregistrare și/sau de autentificare în Sistem. Dacă nu sunteți de acord cu oricare dintre prevederile prezențelor Termenii MyIute sau dacă refuzați prelucrarea datelor dumneavoastră cu caracter personal, astfel cum v-a fost adusă la cunoștință prin Politica de prelucrare a datelor cu caracter personal a O.C.N. „IuteCredit” S.R.L. de pe pagina web a Companiei: <https://iute.md/politica-de-confidentialitate/>, vă rugăm să nu accesați, să nu navigați și să nu utilizați aplicația, nici serviciile, informațiile, materialele și alt conținut cuprins în aceasta.

5. La prima autentificare reușită în Sistem, pentru a putea utiliza funcționalitățile acestuia, Utilizatorul urmează să ia cunoștință de Termenii MyIute și să îi accepte.

6. Acceptarea Termenilor MyIute are loc prin apăsarea butonului „Continuă”, prin care vă exprimați consimțământul pentru utilizarea Sistemului MyIute în condițiile stabilite în Termenii MyIute și în Politica de prelucrare a datelor cu caracter personal a O.C.N. „IuteCredit” S.R.L. Compania își rezervă dreptul ca, în orice moment și la discreția sa exclusivă, să modifice și/sau să înceteze, temporar sau definitiv, Sistemul MyIute (sau o parte din funcționalitățile acestuia), cu sau fără notificarea Clientului. Compania nu va răspunde față de Client și/sau față de terți pentru nicio modificare, suspendare sau încetare a serviciului prestat prin intermediul aplicației. În cazul în care Clientul nu respectă Termenii MyIute, accesul la serviciul din cadrul Sistemului poate fi suspendat și/sau blocat de către Companie, fără notificarea Clientului și fără plata vreunei despăgubiri în favoarea acestuia.

7. Pentru a utiliza Sistemul, trebuie să aveți vârsta de cel puțin 18 ani și să dispuneți de capacitate de exercițiu deplină pentru a vă exprima consimțământul cu privire la prezenții Termenii.

iute Moldova



Chișinău,
Ștefan cel Mare și Sfânt, 182



iute.md
022 801 500



8. Prin apăsarea butonului „Continuă”, declarați și garantați următoarele:

- că aveți dreptul, împuternicirea și capacitatea de exercițiu deplină de a accesa și de a utiliza aplicația;
- că sunteți de acord cu Termenii MyIute și înțelegeți că aceștia vă sunt opozabili;
- că ați fost informat cu privire la condițiile de prelucrare a datelor cu caracter personal stabilite în Politica de prelucrare a datelor cu caracter personal a O.C.N. „IuteCredit” S.R.L., publicată pe pagina web a Companiei, și că sunteți de acord cu aceasta;
- că, prin utilizarea Sistemului MyIute, nu veți încălca nicio lege sau reglementare a Republicii Moldova și că sunteți singurul responsabil de respectarea tuturor legilor și reglementărilor locale aplicabile.

9. În cazul desfășurării unor campanii și promoții, se pot aplica termenii și condițiile speciale ale acestora. Astfel de termeni și condiții pot fi prezentate în formă succintă în cadrul Sistemului, pe pagina web a unui comerciant sau la un punct de activitate al Companiei ori al comerciantului.

10. Persoana care a împlinit vârsta de 18 ani și care deține un număr de identificare de stat al persoanei fizice (IDNP) valabil, atribuit în Republica Moldova, poate iniția crearea profilului în aplicația mobilă MyIute. Profilul se creează doar după verificarea electronică reușită a identității. Pentru a stabili o relație de afaceri, a semna un contract sau a obține acces la produse ori servicii reglementate, solicitantul trebuie să parcurgă cu succes cerințele de onboarding aplicabile, inclusiv verificarea electronică a identității, măsurile de precauție privind clienții, screeningul AML/CFT și clasificarea riscului asociat clientului. Compania poate refuza, suspenda, restricționa sau escala procesul în cazul în care verificarea eșuează, informațiile sunt incomplete, rezultatele screeningului sau ale evaluării riscului necesită examinare ori dacă legislația aplicabilă sau normele interne AML/CFT impun acest lucru.

11. Termenii MyIute au caracter juridic obligatoriu și produc efecte din momentul accesării Sistemului, ambele părți obligându-se să îi respecte la utilizarea și, respectiv, la prestarea serviciilor IuteCredit prin intermediul Sistemului MyIute.

II. NOȚIUNI:

a) **Client sau Utilizator** – persoana fizică aflată în proces de stabilire a unei relații de afaceri cu Compania sau care a stabilit deja o astfel de relație și/sau care a descărcat, a instalat, a accesat și/sau utilizează Sistemul MyIute.

b) **Date cu caracter personal** – orice informație referitoare la o persoană fizică identificată sau identificabilă (subiect al datelor cu caracter personal). Persoană identificabilă este persoana care poate fi identificată.

c) **Sistemul MyIute** – sistem informațional securizat cu acces la distanță, accesibil prin intermediul unui dispozitiv care funcționează pe sistemul de operare iOS sau Android, conectat la internet, disponibil în Google Play și App Store. Dispozitivul utilizat trebuie să fie compatibil cu Sistemul. Sistemul este destinat exclusiv uzului privat și personal. Prin intermediul Sistemului

iute Moldova



Chișinău,
Ștefan cel Mare și Sfânt, 182



iute.md
022 801 500



MyIute, Clienții Companiei pot accesa online contul lor de credit, pot efectua anumite tranzacții și/sau pot contracta la distanță anumite servicii, prin internet, fără a fi necesară prezența fizică la o subdiviziune a Companiei. Accesul la funcționalități și disponibilitatea acestora pot varia în funcție de tipul serviciilor oferite și de politica Companiei la momentul respectiv. Anumite funcționalități pot fi puse la dispoziție și printr-o interfață web; accesul la această interfață se confirmă prin aplicația mobilă MyIute înregistrată pe dispozitivul Clientului. Sistemul MyIute este utilizat și de solicitanții care nu au stabilit încă o relație de afaceri cu Compania, în scopul creării profilului și al parcurgerii procesului de onboarding.

d) **Cod de acces (passcode)** – cod numeric confidențial, ales de Client și utilizat ca parte a mecanismului de autentificare strictă a clientului, legat de dispozitiv, pentru autentificare, aprobare și semnarea contractelor. În componenta hardware securizată a dispozitivului înregistrat se generează o pereche de chei criptografice; cheia privată rămâne pe acel dispozitiv și este protejată prin codul de acces. Acolo unde este activată, deblocarea credențialei se poate efectua prin datele biometrice ale dispozitivului. Codul de acces nu trebuie divulgat niciunui terț. Codul de acces este format din șase cifre și este stabilit și confirmat de Client în aplicația mobilă. Certificatul asociat perechii de chei este emis de serviciul de certificare al Companiei și este revocat la resetarea codului de acces sau la schimbarea dispozitivului înregistrat.

e) **Soluția informatică de identificare la distanță „Digital Onboarding”** – ansamblul elementelor tehnologice utilizate în cadrul aplicației mobile MyIute pentru realizarea procesului de identificare electronică a persoanelor fizice, cetățeni ai Republicii Moldova, deținători ai numărului de identificare de stat al persoanei fizice (IDNP), cu vârsta de cel puțin 18 ani, în scopul onboardingului (inițierii relației de afaceri cu Compania/actualizării datelor acesteia) și al beneficierii de produsele și serviciile specifice oferite de Companie. Această soluție permite transmiterea, prelucrarea și validarea automată a datelor de identificare, a imaginilor actului de identitate și ale chipului Utilizatorului, captate în timp real în cadrul aplicației, precum și a informațiilor comunicate de Utilizator, în scopul verificării identității acestuia fără prezența fizică. Procesul presupune și verificarea datelor furnizate în raport cu informațiile disponibile în Registrul de stat al populației și în alte surse oficiale, în conformitate cu cerințele legale privind prevenirea spălării banilor, combaterea finanțării terorismului, identificarea persoanelor expuse politic și verificarea informațiilor declarate cu privire la rezidența fiscală, precum și cu Regulamentul Băncii Naționale a Moldovei nr. 281/2024 privind cerințele pentru identificarea și verificarea identității clienților prin mijloace electronice. Soluția nu permite utilizarea fotografiilor sau a înregistrărilor video realizate anterior; imaginile actului de identitate și ale chipului Utilizatorului sunt captate în timp real, în cadrul aplicației, și sunt supuse verificărilor de detectare a mișcării/vitalității (liveness).

f) **Termenii MyIute** – Termenii și condițiile de utilizare a Sistemului MyIute stabiliți în prezentul document constituie contractul juridic încheiat între Companie și Client. Termenii MyIute stabilesc modul în care Clienții pot fi supuși onboardingului (pot iniția o relație de afaceri cu Compania), își pot actualiza datele și pot utiliza Sistemul MyIute pentru a beneficia de produsele și serviciile specifice oferite de Companie.



III. AUTENTIFICAREA ÎN MYIUTE:

12. Accesul la Sistemul MyIute se inițiază prin introducerea numărului de identificare de stat al persoanei fizice (IDNP). În acest scop, Clientul trebuie să dețină un număr de telefon mobil declarat Companiei, conectat la unul dintre operatorii de telefonie mobilă din Republica Moldova și apt de a recepționa mesaje SMS, precum și, în cazul în care a fost configurată autentificarea strictă a clientului, dispozitivul mobil înregistrat în Sistemul MyIute.

13. Pentru a utiliza Sistemul MyIute, trebuie să fiți persoană fizică, cu vârsta de cel puțin 18 ani, deținătoare a unui act de identitate valabil și a unui număr de identificare de stat al persoanei fizice (IDNP) atribuit în Republica Moldova. Sistemul MyIute poate fi utilizat exclusiv pentru efectuarea operațiunilor în nume propriu.

14. Pentru ca Compania să își execute obligațiile ce decurg din Legea nr. 308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, din Regulamentul Băncii Naționale a Moldovei nr. 281/2024 privind cerințele pentru identificarea și verificarea identității clienților prin mijloace electronice și din Legea nr. 195/2024 privind protecția datelor cu caracter personal, Compania prelucrează date cu caracter personal în scopul identificării Clientului și al autentificării acestuia în Sistemul MyIute, al asigurării securității tranzacțiilor și al aplicării măsurilor de precauție pentru prevenirea furtului de identitate online.

15. Sistemul poate fi utilizat doar dacă dispozitivul folosit pentru accesarea acestuia este securizat prin parolă, amprentă digitală, Face ID sau altă metodă de securitate oferită de dispozitiv.

16. Scopul Sistemului MyIute este implementarea unei metode sigure de identificare a Clienților în cadrul sistemului, garantând astfel Utilizatorilor un nivel sporit de securitate, facilitând accesul Clienților la Sistem de la distanță și permițând Clientului să efectueze operațiuni frecvente la distanță, în siguranță și fără prezență fizică.

17. Înregistrarea Utilizatorului se efectuează de către Companie prin aplicarea procedurii sale de autentificare (login) a Clientului. Înregistrarea presupune prelucrarea anumitor date cu caracter personal, astfel cum v-a fost adusă la cunoștință prin Politica de prelucrare a datelor cu caracter personal a O.C.N. „IuteCredit” S.R.L. de pe pagina web a Companiei. După autentificarea în Sistem, Utilizatorului i se solicită să creeze un cod de acces din șase cifre și, opțional, să activeze deblocarea biometrică; prin aceste acțiuni, Utilizatorul configurează totodată autentificarea strictă a clientului, adică stabilește mecanismul prin care Compania îi validează în siguranță identitatea. Stabilirea codului de acces este precedată de verificarea electronică a identității. La stabilirea codului de acces, în componenta hardware securizată a dispozitivului se generează o pereche de chei criptografice: cheia privată rămâne pe dispozitiv, protejată prin codul de acces, și nu îl părăsește niciodată, iar certificatul corespunzător este emis de serviciul de certificare al Companiei și înregistrat pentru dispozitivul respectiv. Deblocarea biometrică, atunci când este activată de Utilizator, doar deblochează cheia protejată prin codul de acces și nu înlocuiește codul de acces.

18. Accesul la MyIute este asociat Utilizatorului înregistrat și, în cazul autentificării stricte a clientului legate de dispozitiv, unui singur dispozitiv mobil înregistrat la un moment dat. Un dispozitiv înregistrat nu poate fi utilizat ca dispozitiv MyIute activ pentru mai mulți Utilizatori, iar un Utilizator



nu poate utiliza MyIute simultan pe mai multe dispozitive active. La schimbarea dispozitivului sau la resetarea codului de acces, Compania poate solicita verificarea numărului de telefon și repetarea verificării electronice a identității, poate revoca credențialele anterioare, poate dezactiva înregistrarea dispozitivului precedent și poate emite o nouă credențială legată de dispozitiv. Înainte de efectuarea schimbării dispozitivului, Utilizatorul este avertizat că înregistrarea de pe dispozitivul anterior va fi dezactivată și trebuie să confirme schimbarea.

18A. Autentificarea în aplicația mobilă poate impune Utilizatorului deblocarea cheii private legate de dispozitiv prin codul de acces sau printr-o metodă biometrică activată, precum și semnarea unei provocări criptografice de unică folosință. Accesul web, acolo unde este pus la dispoziție, poate necesita aprobarea prin aplicația mobilă MyIute înregistrată, inclusiv potrivirea numărului afișat, confirmarea prin codul de acces sau biometric și un răspuns semnat de dispozitiv, limitat în timp. Provocările eșuate, expirate, anulate sau neconcordante pot fi respinse și pot declanșa blocarea accesului sau alte controale de securitate. În cazul în care codul de acces nu a fost încă stabilit, accesul prin interfața web nu poate fi finalizat; Utilizatorul este direcționat către aplicația mobilă, prin intermediul unui cod QR sau al unui link de descărcare, pentru a efectua verificarea identității și a stabili codul de acces. Compania aplică termene de valabilitate, limite privind numărul de încercări și blocări temporare în privința parolelor de unică folosință, a cererilor de confirmare și a introducerii codului de acces.

18B. În cazul în care Utilizatorul resetează codul de acces uitat sau schimbă dispozitivul înregistrat, se aplică următorii pași: verificarea deținerii numărului de telefon declarat prin intermediul unei parole de unică folosință; repetarea verificării electronice a identității, prin actul de identitate și verificarea biometrică; dezactivarea înregistrării dispozitivului anterior, după caz; stabilirea unui nou cod de acces. În cazul în care verificarea identității nu este reușită, resetarea este refuzată, iar accesul la Sistemul MyIute nu este acordat.

18C. Contractele, cererile și alte documente puse la dispoziție în Sistemul MyIute sunt semnate de Utilizator prin introducerea codului de autentificare de unică folosință transmis prin SMS. Prin acceptarea Termenilor MyIute, Utilizatorul este de acord că aplicarea în acest mod a codului de autentificare transmis prin SMS constituie semnătura electronică a Utilizatorului, că aceasta produce efectele juridice convenite între părți și că Compania este în drept să se prevaleze de aceasta ca dovadă a consimțământului Utilizatorului. Documentele pot fi semnate în Sistemul MyIute exclusiv în nume propriu.

19. Datele Utilizatorului, inclusiv cele furnizate în formularul „Cunoaște-ți clientul”, trebuie să fie veridice și actualizate pentru a putea accesa Sistemul.

20. Pentru a utiliza Sistemul, Utilizatorul trebuie să îi permită accesul la anumite funcții ale dispozitivului, necesare pentru buna funcționare a Sistemului MyIute. Utilizarea Sistemului echivalează cu acordul Utilizatorului privind accesul Sistemului MyIute la funcțiile dispozitivului. Astfel de funcții includ, în special, accesul la cameră, în scopul captării actului de identitate și a imaginii faciale, precum și accesul la componenta hardware securizată a dispozitivului, în scopul generării și stocării credențialelor de autentificare și al confirmării autentificărilor și operațiunilor. În

iute Moldova



Chișinău,
Ștefan cel Mare și Sfânt, 182



iute.md
022 801 500



conformitate cu cerințele de reglementare aplicabile, Compania colectează și păstrează totodată datele tehnice ale dispozitivului utilizat, inclusiv modelul și parametrii dispozitivului, versiunea aplicației și a sistemului de operare, adresa IP și datele de conexiune la rețea, fusul orar și setările de limbă, în scopurile identificării, prevenirii fraudei și securității procesului.

21. Clientul acceptă și înțelege că îi revine responsabilitatea de a păstra confidențialitatea datelor de autentificare asociate utilizării Sistemului și de a lua măsuri rezonabile pentru menținerea confidențialității acestor informații.

22. Profilurile Utilizatorilor nu sunt transferabile către niciun terț.

23. Utilizatorul trebuie să se asigure că informațiile incluse în profil sunt actualizate, complete, exacte și fiabile.

24. Clientul se obligă să notifice Compania de îndată, fără întârzieri nejustificate, din momentul în care a luat cunoștință de pierderea, sustragerea, însușirea ilegală sau utilizarea neautorizată a datelor sale de autentificare, precum și a telefonului mobil utilizat pentru accesarea aplicației. De asemenea, sunteți de acord să notificați Compania de îndată, fără întârzieri nejustificate, în același mod, cu privire la orice altă încălcare a securității legată de serviciile prestate prin intermediul Sistemului, de care luați cunoștință.

IV. CONDIȚII GENERALE DE UTILIZARE A SOLUȚIEI INFORMATICE DE IDENTIFICARE LA DISTANȚĂ „DIGITAL ONBOARDING”:

25. Onboardingul digital este un proces desfășurat la distanță prin intermediul aplicației mobile MyIute. Acesta poate include: colectarea și verificarea IDNP-ului, a numărului de telefon și a adresei de poștă electronică ale Utilizatorului; verificarea numărului de telefon printr-o parolă de unică folosință din șase cifre, transmisă prin SMS și valabilă o perioadă limitată; verificarea electronică a identității prin intermediul unei soluții e-KYC integrate, aparținând unui terț, inclusiv captarea și verificarea actului de identitate și verificările biometrice/de vitalitate (liveness); configurarea autentificării stricte a clientului legate de dispozitiv; colectarea sau confirmarea informațiilor privind adresa oficială și adresa de reședință, naționalitatea, locul nașterii, rezidența fiscală și cetățenia; completarea chestionarului aplicabil privind măsurile de precauție referitoare la client; examinarea și confirmarea datelor colectate; screeningul AML/CFT și clasificarea riscului; precum și, atunci când este necesar, examinarea manuală de către Companie.

- **Statutul profilului și al cererii.** În cursul onboardingului pot fi stocate fișa clientului sau cererea de produs în formă de proiect, însă procesarea cererii și decizia de creditare nu au loc până la parcurgerea cu succes a cerințelor de onboarding.

- **Chestionarul de precauție privind clientul (CDD).** Utilizatorului i se solicită să furnizeze informații care includ statutul de persoană expusă politic sau de persoană asociată acesteia, scopul relației de afaceri, sursa veniturilor, statutul ocupațional și sectorul de activitate. Chestionarul și variantele de răspuns pot varia în funcție de țară, de nivelul de risc al clientului și de versiunea activă configurată de Companie.

- **Screeningul și evaluarea riscului.** Compania evaluează Utilizatorul în funcție de risc, utilizând datele clientului, răspunsurile din chestionar, screeningul în listele de sancțiuni, în listele privind persoanele expuse politic și în sursele media negative, precum și alte informații permise. Rezultatele care indică un risc redus pot fi aprobate automat; rezultatele care indică un risc sporit, un risc inacceptabil sau care sunt semnalate în alt mod pot fi transmise spre examinare manuală, pot rămâne în așteptare, pot fi respinse sau pot conduce, după caz, la blocarea definitivă.
- **Verificarea numărului de telefon.** Numărul de telefon declarat de Utilizator se verifică prin intermediul unei parole de unică folosință (OTP) din șase cifre, transmisă prin SMS, valabilă timp de trei minute. În cazul în care codul nu este introdus în acest interval, acesta este invalidat, iar Utilizatorul urmează să solicite transmiterea unui nou cod sau să reia procesul. Procedura la distanță poate fi finalizată doar în cazul în care parola de unică folosință a fost transmisă și validată. Fișa Clientului se creează în sistemele Companiei doar după verificarea reușită a numărului de telefon.
- **Verificarea electronică a identității.** Verificarea se realizează prin soluția e-KYC integrată în aplicația mobilă, operată de un prestator specializat contractat de Companie. Aceasta presupune consimțământul prealabil al Utilizatorului, acordarea accesului la cameră, captarea în timp real a ambelor fețe ale actului de identitate și a imaginii faciale, verificările de detectare a mișcării/vitalității (liveness), verificarea automată a autenticității și valabilității documentului, compararea imaginii faciale cu fotografia din document și confruntarea datelor cu Registrul de stat al populației. Rezultatul este transmis Companiei în formă semnată digital și este verificat de Companie înainte de a fi înregistrat.
- **Adresa și informațiile cu caracter personal.** Datele privind adresa oficială sunt precompletate în baza răspunsului recepționat din registrul de stat, iar Utilizatorul le confirmă sau le completează și poate declara o adresă de reședință diferită. Utilizatorul furnizează totodată informații privind naționalitatea, locul nașterii, rezidența fiscală și cetățenia.
- **Examinarea datelor.** Înainte de transmiterea datelor spre evaluare, Utilizatorului îi sunt prezentate toate datele colectate pe parcursul onboardingului, acesta putând fie să le confirme, fie să revină pentru a le corecta.
- **Semnarea contractului și accesul la produs.** În cazul încheierii unui contract, acesta se semnează prin codul de autentificare de unică folosință transmis prin SMS, iar accesul la produs sau serviciu se acordă doar după parcurgerea cu succes a onboardingului de către Utilizator și semnarea contractului.

26. Pentru a garanta siguranța și transparența serviciilor noastre, Compania aplică proceduri stricte de identificare tuturor persoanelor care inițiază o relație de afaceri cu Compania prin canale electronice, în deplină conformitate cu legislația Republicii Moldova privind prevenirea și combaterea spălării banilor și finanțării terorismului (AML/CFT) și cu Regulamentul Băncii Naționale a Moldovei nr. 281/2024 privind cerințele pentru identificarea și verificarea identității clienților prin mijloace electronice.

iute Moldova



Chișinău,
Ștefan cel Mare și Sfânt, 182



iute.md
022 801 500



26A. Înainte de accesarea soluției de identificare la distanță, Compania pune la dispoziția Utilizatorului prezenții Termeni MyIute, nota de informare privind prelucrarea și protecția datelor cu caracter personal, precum și versiunea rezumativă a politicii sale privind prevenirea spălării banilor și finanțării terorismului, care descrie identificarea Clientului, măsurile de precauție aplicate și tratamentul persoanelor expuse politic. Procesul de identificare electronică este precedat de consimțământul Utilizatorului privind prelucrarea datelor cu caracter personal, inclusiv a datelor biometrice.

27. Fiecare solicitant parcurge un proces de identificare electronică, în cadrul căruia se aplică următoarele măsuri:

- verificarea valabilității și autenticității actului de identitate;
- colectarea, după caz, a altor informații relevante, în funcție de cerințele legale și de profilul de risc al Clientului;
- evaluarea automată a informațiilor furnizate de Utilizator, în scopul stabilirii identității reale a acestuia;
- verificarea numărului de telefon și a adresei de poștă electronică prin intermediul unei parole de unică folosință, fără validarea căreia procesul nu poate fi finalizat;
- captarea în timp real a actului de identitate, pe ambele fețe, și a imaginii faciale, împreună cu verificările de detectare a mișcării/vitalității (liveness); încărcarea fotografiilor sau a înregistrărilor video realizate anterior nu este permisă;
- verificarea automată a elementelor de securitate, a designului și a zonei citibile optic a documentului, precum și compararea imaginii faciale cu fotografia din actul de identitate;
- confruntarea datelor declarate cu datele disponibile în Registrul de stat al populației;
- verificarea solicitantului în listele de sancțiuni internaționale și ale Uniunii Europene, în listele privind terorismul și proliferarea armamentului, sub aspectul statutului de persoană expusă politic, precum și în raport cu informațiile din surse publice credibile;
- înregistrarea și păstrarea datelor tehnice ale dispozitivului utilizat, precum și a imaginilor și informațiilor captate pe parcursul procesului;
- Datele furnizate sunt prelucrate în condiții de securitate maximă și sunt utilizate exclusiv în scopul identificării și verificării Clientului, al evaluării riscului asociat acestuia și al respectării obligațiilor legale.

27A. Compania nu inițiază relația de afaceri prin mijloace electronice în cazul în care nu pot fi aplicate măsurile standard de precauție privind clienții, în care nu sunt întrunite cerințele tehnice ale soluției de identificare sau în care identitatea solicitantului nu poate fi verificată. În astfel de cazuri, identificarea electronică se consemnează ca nereușită, procesul de onboarding nu se

finalizează, iar solicitantul poate fi invitat să inițieze relația de afaceri în prezența unui reprezentant al Companiei.

27B. În cazul în care există suspiciuni privind existența unui viciu de consimțământ, inclusiv exercitarea unor presiuni fizice sau psihologice asupra solicitantului, ori alte suspiciuni referitoare la procesul de identificare, Compania va solicita prezența fizică a solicitantului la una dintre subdiviziunile sale. În cazul în care există îndoieli privind veridicitatea datelor sau a documentelor prezentate, Compania poate solicita informații ori confirmări suplimentare sau aplicarea semnăturii electronice pe copia actului de identitate.

28. Compania respectă cu strictețe normele AML/CFT, inclusiv:

- identificarea și monitorizarea persoanelor expuse politic (PEP), a membrilor familiilor acestora și a persoanelor cunoscute ca fiind asociate acestora;
- aplicarea măsurilor de precauție în funcție de tipul relației de afaceri și de tranzacțiile efectuate.
- În cazul în care solicitantul declară sau în care screeningul indică faptul că acesta este persoană expusă politic, membru al familiei unei astfel de persoane ori persoană cunoscută ca fiind asociată acesteia, se aplică măsuri sporite de precauție privind clienții, iar dosarul se transmite spre examinare manuală și spre decizia funcției autorizate de risc și conformitate a Companiei. De asemenea, Compania poate solicita ca relația de afaceri să fie inițiată prin prezență fizică la una dintre subdiviziunile sale, în baza unei evaluări individuale.

29. Informațiile furnizate de Client sunt colectate și stocate în sisteme informaționale securizate, accesibile doar personalului autorizat și utilizate exclusiv în scopurile permise de lege. Compania nu va divulga informațiile către terți, cu excepția situațiilor expres prevăzute de cadrul legal aplicabil sau în temeiul unui temei juridic justificat. Documentele și informațiile obținute în cadrul identificării electronice, inclusiv imaginile captate, copiile actelor de identitate, datele tehnice ale dispozitivului utilizat și adresa IP, se păstrează pe întreaga perioadă a relației de afaceri și timp de cinci ani de la încetarea acesteia și se pun la dispoziție, la cerere, Băncii Naționale a Moldovei, Serviciului Prevenirea și Combaterea Spălării Banilor și organelor de drept.

30. Clientul este obligat să furnizeze informații corecte, complete și veridice la toate etapele procesului de identificare și să își actualizeze datele cu caracter personal la solicitarea Companiei sau ori de câte ori intervin modificări. Prin acceptarea Termenilor MyIute, confirmați că toate informațiile furnizate sunt veridice și că mijloacele financiare utilizate în relația cu Compania provin din surse legale.

30A. După completarea chestionarului de precauție privind clientul, Compania stabilește automat nivelul de risc al Clientului, prin intermediul unui motor decizional intern, în baza unor criterii ponderate configurate în setările sale AML/CFT. Criteriile includ, în special, rezidența fiscală, adresa oficială, locul nașterii, cetățenia și vârsta Clientului, metoda de onboarding utilizată, răspunsurile oferite în chestionar (statutul de persoană expusă politic sau de persoană asociată



acesteia, sursa veniturilor, scopul relației de afaceri, statutul ocupațional și sectorul de activitate), precum și rezultatele screeningului efectuat în listele de sancțiuni, în listele persoanelor expuse politic și în sursele media negative. Clientul este încadrat în unul dintre următoarele niveluri de risc: redus, redus spre mediu, mediu, mediu spre sporit, sporit sau inacceptabil.

31. Compania aplică măsuri continue de precauție privind clienții, în funcție de risc, pe întreg ciclul de viață al relației cu clientul, indiferent dacă acesta are sau nu un credit în derulare. La autentificare și la survenirea unor evenimente relevante, Compania poate verifica dacă verificarea identității a fost finalizată, dacă Clientul deține un chestionar de precauție valabil, dacă data de reînnoire aplicabilă a expirat sau se apropie, precum și dacă alți factori declanșatori impun actualizarea informațiilor, inclusiv expirarea datelor de identificare, modificarea profilului de risc, depunerea unei noi cereri de produs sau indicii privind o activitate suspectă ori neobișnuită.

31A. În cazul în care chestionarul de precauție privind clientul sau actualizarea necesară a datelor clientului a expirat, Clientul trebuie să completeze sau să confirme informațiile solicitate înainte de a continua utilizarea aplicației MyIute, iar accesul poate fi restricționat până la finalizarea acestora. În cazul în care se apropie termenul de reînnoire, Compania îi poate propune Clientului o actualizare anticipată, cu caracter opțional. Momentul și conținutul solicitărilor de reînnoire pot varia în funcție de clasificarea curentă a riscului Clientului, de cerințele de reglementare și de setările AML/CFT ale Companiei. În cazul în care Clientul nu a parcurs anterior verificarea electronică a identității, chestionarul nu este solicitat până la finalizarea acestei verificări. În cazul în care chestionarul expiră în următoarele 30 de zile, completarea acestuia este propusă ca etapă opțională, pe care Clientul o poate amâna. Termenul de valabilitate a chestionarului este stabilit pentru fiecare nivel de risc în setările AML/CFT ale Companiei, iar perioada premergătoare expirării poate fi modificată de Companie.

31B. Informațiile privind screeningul și riscul pot fi recepționate în mod asincron de la prestatori de servicii specializați. În cazul în care rezultatele ulterioare indică un nivel de risc mai ridicat sau impun în alt mod anumite acțiuni, Compania poate actualiza clasificarea Clientului, poate iniția o examinare de conformitate, poate solicita informații suplimentare, poate restricționa accesul sau serviciile, poate respinge riscul ori poate lua alte măsuri permise de lege și de normele interne AML/CFT. Compania realizează totodată monitorizarea continuă a relației de afaceri și a tranzacțiilor, inclusiv prin mijloace automatizate, în scopul identificării operațiunilor neobișnuite sau suspecte. În cazul în care sunt identificate suspiciuni de spălare a banilor sau de finanțare a terorismului, Compania informează Serviciul Prevenirea și Combaterea Spălării Banilor, în conformitate cu legea, și nu este în drept să informeze Clientul despre aceasta.

31C. Clienților identificați și supuși onboardingului de către Companie înainte de intrarea în vigoare a procesului de precauție privind clienții descris în prezentul Capitol li se va solicita completarea chestionarului de precauție la prima autentificare ulterioară în aplicația MyIute.

32. Compania își rezervă dreptul de a restricționa accesul la Digital Onboarding pentru persoanele fizice din anumite jurisdicții considerate cu risc sporit din perspectiva reglementărilor

AML/CFT sau supuse sancțiunilor internaționale.

33. Compania nu stabilește relații de afaceri cu persoane sau entități implicate în finanțarea terorismului, incluse în listele de sancțiuni internaționale ori care prezintă un nivel inacceptabil de risc din perspectiva reglementărilor AML/CFT.

34. Compania poate refuza inițierea sau poate înceta relația contractuală în orice moment, în cazul unor suspiciuni rezonabile privind legalitatea mijloacelor financiare, scopul relației sau exactitatea informațiilor furnizate, precum și din alte motive justificate potrivit politicilor sale interne.

34A. Compania consemnează etapa la care a ajuns fiecare solicitant sau Client în procesul de onboarding prin intermediul unui statut de onboarding. Doar Clientul care deține statutul de client integral supus onboardingului poate încheia un contract cu Compania și poate beneficia de produsele și serviciile puse la dispoziție în Sistemul MyIute. Pot fi aplicate următoarele statute: (i) onboardat – sunt disponibile toate datele și verificările impuse de normele aplicabile, iar Clientul poate intra într-o relație contractuală cu Compania; (ii) onboardat inițial – Client potențial care nu deține toate datele necesare pentru a intra într-o relație contractuală; (iii) verificare nereușită – verificarea electronică a identității nu a fost reușită; (iv) onboarding în așteptare – dosarul se află în așteptarea finalizării activităților de precauție privind clientul, precum examinarea unei verificări AML/CFT sau a evaluării riscului; (v) risc neacceptat – riscul asociat Clientului nu a fost acceptat, acest statut putând fi modificat doar manual și în urma unei noi evaluări; și (vi) inclus în lista neagră – Clientul este exclus definitiv, de exemplu în cazul în care acesta este supus sancțiunilor internaționale sau în care a fost constatată o fraudă.

35. Compania poate utiliza soluția informatică de identificare la distanță „Digital Onboarding” și pentru actualizarea datelor Clienților.

35A. În scopul desfășurării procesului de onboarding și al aplicării măsurilor continue de precauție privind clienții, Compania recurge la prestatori de servicii specializați, în special pentru verificarea electronică a identității, pentru screeningul și monitorizarea în scopuri AML/CFT, pentru transmiterea mesajelor SMS, pentru emiterea certificatelor și pentru găzduirea sistemelor informaționale. Acești prestatori acționează în baza unui contract încheiat cu Compania și în conformitate cu instrucțiunile acesteia, Compania rămânând responsabilă de respectarea cerințelor aplicabile identificării și verificării identității Clienților prin mijloace electronice.

V. FUNCȚIONALITĂȚILE SISTEMULUI MYIUTE:

36. Sistemul MyIute oferă, fără a se limita la acestea, următoarele funcționalități:

- onboardingul digital al Clientului prin soluția informatică de identificare la distanță „Digital Onboarding”;
- actualizarea datelor Clientului prin soluția informatică de identificare la distanță „Digital Onboarding”;
- recepționarea în timp real a notificărilor din partea Companiei privind diverse tranzacții și activități financiare, precum și actualizările contului;

- instalarea aplicației prin Google Play/App Store;
- depunerea unei cereri de credit, care poate fi stocată în formă de proiect pe parcursul onboardingului; interogările registrelor de venituri și de credite, evaluarea cererii și decizia de creditare se inițiază doar după parcurgerea cu succes a onboardingului de către Utilizator;
- achiziționarea unei polițe de asigurare;
- deconectarea/blocarea Clientului Companiei din MyIute în cazul în care acesta încalcă regulile de efectuare a operațiunilor prin MyIute;
- posibilitatea de a lua cunoștință de ofertele curente ale Companiei.
- completarea chestionarului de precauție privind clientul și actualizarea datelor Clientului;
- stabilirea, modificarea și resetarea codului de acces, precum și gestionarea dispozitivului înregistrat;
- semnarea contractelor și a altor documente prin intermediul codului de autentificare de unică folosință transmis prin SMS;
- confirmarea autentificărilor efectuate prin interfața web, acolo unde aceasta este pusă la dispoziție.

37. Compania își revizuiește periodic oferta de funcționalități digitale. Funcționalitățile disponibile la această dată pot fi completate cu altele noi și vor fi comunicate în Manualul de utilizare a Sistemului MyIute. Unele funcționalități pot fi restricționate/excluse din oferta digitală a Companiei, în orice moment, pentru orice motiv, cu sau fără notificare. Unele funcționalități sunt accesibile doar în cadrul zilei operaționale.

41. Funcționalitățile disponibile prin intermediul Sistemului pot oferi posibilitatea de a încărca, publica, descărca sau transmite conținut. În acest caz, Utilizatorul este responsabil de conținutul pe care l-a încărcat, publicat, descărcat sau transmis prin intermediul Sistemului.

42. Compania își rezervă dreptul de a elimina sau de a refuza publicarea conținutului care încalcă Termenii MyIute ori cadrul de reglementare aplicabil, acest fapt neînsemnând însă că monitorizează, analizează sau verifică în mod continuu vreun conținut.

VI. DREPTURILE ȘI OBLIGAȚIILE PĂRȚILOR:

43. În calitate de Client existent al Companiei, aveți următoarele drepturi:

- să primiți consultanță în cazul oricăror neclarități, contactând Serviciul Suport Clienți în orele de program stabilite pentru zilele lucrătoare;
- să modificați sau să resetați codul de acces și să activați ori să dezactivați deblocarea biometrică, cu condiția verificării numărului de telefon declarat și a repetării verificării electronice a identității;

iute Moldova



Chișinău,
Ștefan cel Mare și Sfânt, 182



iute.md
022 801 500



– să încetați, în orice moment după acceptarea prezenților Termeni MyIute, utilizarea Sistemului MyIute.

44. Totodată, sunteți obligat:

- să nu furnizați Companiei date false, incorecte sau neactualizate, care ar putea induce în eroare sistemul Companiei;
- să nu introduceți date cu caracter personal incorecte sau care nu vă aparțin. Utilizarea frauduloasă a datelor cu caracter personal ale altei persoane poate atrage răspunderea contravențională sau penală;
- să mențineți o metodă de deblocare a telefonului pe toată durata în care Sistemul MyIute este instalat pe acesta;
- să nu accesați linkuri, să nu instalați aplicații și să nu răspundeți la mesaje sau apeluri prin care vi se solicită date cu caracter personal ori informații confidențiale. De asemenea, nu instalați aplicații de control la distanță sau orice alte aplicații ori actualizări din surse necunoscute, actualizări neoficiale sau orice program care ar putea permite accesul neautorizat la dispozitivul dumneavoastră mobil, la credențialele sau la conturile dumneavoastră. În cazul încălcării acestor obligații sau în cazul în care unui terț i se permite, intenționat ori din neglijență, accesul la dispozitiv, la datele de autentificare sau la codurile de autorizare ori de securitate ale Utilizatorului, se consideră că Utilizatorul a autorizat terțul respectiv să acționeze în numele și pe contul său. Utilizatorul poartă răspunderea deplină pentru orice tranzacție efectuată prin intermediul Sistemului, inclusiv pentru tranzacțiile, plățile, creditele sau alte operațiuni inițiate de terți prin utilizarea datelor și a accesului divulgate ori compromise;
- să nu divulgați niciunui terț parola/codul de securitate de deblocare a telefonului, întrucât divulgarea acestora vă expune riscului de acces neautorizat la profilul dumneavoastră MyIute și de efectuare a unor operațiuni în numele dumneavoastră. Sunteți singurul responsabil de păstrarea confidențialității și de securitatea datelor introduse în Sistemul MyIute, a parolei/codului de securitate de deblocare a telefonului, a codului de acces și a codului OTP. De asemenea, răspundeți pentru orice activități, de orice natură, care au loc pe cont;
- să nu permiteți înregistrarea pe telefon a datelor biometrice (amprente digitale sau Face ID) ale altor persoane, în cazul în care activați datele biometrice pentru autentificarea în Sistemul MyIute, având în vedere că, într-un astfel de caz, accesul la Sistem și autorizarea tranzacțiilor s-ar putea efectua prin oricare dintre datele biometrice adăugate pe telefon;
- să ne notificați de îndată cu privire la orice utilizare neautorizată a Sistemului instalat pe numărul dumneavoastră personal de telefon sau cu privire la orice încălcare a securității telefonului și/sau a datelor de autentificare în Sistem, de care luați cunoștință ori pe care ar trebui, în mod rezonabil, să o bănuiți;
- să nu divulgați terților codul OTP recepționat pe numărul dumneavoastră personal de telefon, codul de acces sau orice alt cod utilizat pentru autentificare ori pentru semnarea



documentelor în MyIute, întrucât divulgarea acestora permite autorizarea unor operațiuni în numele dumneavoastră;

- să ne notificați cu privire la pierderea, sustragerea sau accesul neautorizat la telefonul mobil pe care este instalat Sistemul MyIute, de îndată ce ați luat cunoștință de o astfel de situație. În cazul în care nu executați obligația menționată mai sus, vă asumați răspunderea deplină pentru toate operațiunile pe care persoanele neautorizate le-ar putea efectua prin intermediul Sistemului MyIute sau ca urmare a identificării realizate prin Sistemul instalat pe numărul de telefon declarat Companiei, în cadrul unui apel către/de la Centrul de Contact al Companiei ori la o unitate a Companiei, inclusiv accesul la orice informație sau actualizarea datelor;

- să dezinstalați Sistemul în cazul în care telefonul pe care l-ați instalat inițial nu vă mai aparține sau în care nu îl veți mai utiliza;

- să nu falsificați și să nu furnizați informații eronate cu privire la identitatea sau intențiile dumneavoastră ori cu privire la orice aspect legat de Sistem;

- să nu transmiteți, să nu distribuiți și să nu oferiți informații sau materiale care sunt, integral ori parțial, ilegale, false, frauduloase sau neadecvate, ofensatoare ori care încalcă ordinea publică și bunele moravuri;

- să confirmați sau să actualizați datele dumneavoastră de identificare, valabilitatea actelor de identitate și alte informații ori de câte ori este necesar, la solicitarea Companiei;

- să asigurați și să mențineți securitatea fizică și logică a telefonului, în conformitate cu recomandările producătorului și cu bunele practici;

- să actualizați sistemul de operare al telefonului în conformitate cu recomandările producătorului și să utilizați doar versiunile oficiale ale sistemului de operare furnizate de producător;

- să nu eludați protecțiile de securitate ale sistemelor de operare recomandate de producătorul telefonului mobil;

- să instalați Sistemul MyIute doar din sursele oficiale ale magazinelor dedicate – Google Play Market sau App Store – publicate la solicitarea Companiei;

- să vă asigurați că datele sunt introduse în Sistem corect și complet;

- să nu încălcați niciun drept prevăzut de lege, niciun drept de proprietate, niciun drept nepatrimonial, dreptul la viață privată sau altele asemenea;

- să nu utilizați conținutul Sistemului pentru a revinde, a distribui sau a folosi în alt mod serviciile oferite în orice alt scop decât cel permis de prezenții Termeni MyIute;

- să nu distribuiți ofertele cuprinse în Sistemul MyIute;



- să nu utilizați abuziv și/sau cu rea-credință și/sau în scopuri frauduloase funcționalitățile oferite în cadrul Sistemului și să nu încercați să le accesați prin orice altă metodă decât prin interfața și instrucțiunile puse la dispoziție de Companie;

- să nu încărcați, să nu accesați, să nu publicați, să nu transmiteți prin poșta electronică și să nu transmiteți în alt mod materiale care conțin viruși sau alt cod informatic, fișiere ori programe destinate să întrerupă, să distrugă sau să limiteze funcționalitatea Sistemului ori a oricărui alt serviciu sau funcționalități electronice disponibile în cadrul Sistemului.

45. Compania își rezervă dreptul:

- de a suspenda temporar sau de a anula contul Clientului în cazul încălcării de către Utilizator a prevederilor prezenților Termeni MyIute ori al altor acțiuni care nu se încadrează în normele și politicile aplicabile;

- de a prelucra datele cu caracter personal în conformitate cu Politica de prelucrare a datelor cu caracter personal a O.C.N. „IuteCredit” S.R.L. de pe pagina web a Companiei: <https://iute.md/politica-de-confidentialitate/>;

- de a verifica și de a modifica/actualiza datele Clienților în vederea respectării cerințelor legale aplicabile activității Companiei;

- de a implementa modificări, îmbunătățiri, actualizări de securitate și remedieri ale erorilor, în vederea optimizării experienței utilizatorului și a asigurării bunei funcționări a Sistemului;

- de a modifica Termenii MyIute, versiunea actualizată a acestora urmând a fi publicată în Sistem și pe pagina web a Companiei. Este responsabilitatea Utilizatorului să citească Termenii MyIute și Politica de prelucrare a datelor cu caracter personal a O.C.N. „IuteCredit” S.R.L. de pe pagina web a Companiei înainte de a utiliza Sistemul. Continuarea utilizării Sistemului după publicarea oricărei modificări sau completări constituie acceptarea acestora de către Utilizator;

- de a actualiza, îmbunătăți sau modifica în alt mod Sistemul în orice moment, pentru orice motiv, cu sau fără notificare. Prezenții Termeni MyIute se aplică tuturor acestor actualizări, îmbunătățiri sau modificări ale Sistemului;

- de a suspenda utilizarea Sistemului pe durata perioadelor de mentenanță (planificată sau neplanificată) ori în cazul unor defecțiuni tehnice sau al altor circumstanțe. În acest caz, operațiunile solicitate de Client pot fi efectuate prin prezență fizică la Companie, în condițiile și cu comisioanele stabilite de Companie pentru astfel de operațiuni.

46. Compania se obligă:

- să asigure protecția și confidențialitatea datelor cu caracter personal;
- să păstreze confidențialitatea informațiilor privind tranzacțiile/operațiunile de plată și conturile Clientului, gestionate de Companie prin intermediul Sistemului MyIute;

iute Moldova



Chișinău,
Ștefan cel Mare și Sfânt, 182



iute.md
022 801 500



- să informeze corespunzător Clientul și să acorde suport în utilizarea Sistemului MyIute;
- să înregistreze/modifice datele Clienților în conformitate cu cerințele reglementărilor interne ale Companiei;
- să recepționeze, să înregistreze și să examineze cererile și solicitările Clienților în orele de program stabilite pentru zilele lucrătoare;
- să blocheze accesul Clientului la Sistem la cererea acestuia, recepționată telefonic sau prin poșta electronică în zilele lucrătoare și în conformitate cu programul de lucru al Companiei;
- să ofere Clienților posibilitatea de a-și retrage consimțământul privind prelucrarea datelor cu caracter personal, în condițiile legii;
- să mențină nivelul optim de securitate și să implementeze toate măsurile necesare pentru protecția datelor personale și financiare ale Utilizatorilor;
- să execute, în numele Clientului, tranzacțiile autorizate de acesta, în conformitate cu programul zilei operaționale pentru prestarea serviciului respectiv, astfel cum este definit în Termenii MyIute.

VII. PRELUCRAREA DATELOR CU CARACTER PERSONAL:

47. Compania, în calitate de operator de date cu caracter personal, prelucrează datele cu caracter personal ale Clienților care doresc să utilizeze Sistemul MyIute în conformitate cu prevederile legale aplicabile în domeniul protecției datelor cu caracter personal și astfel cum este stabilit în Politica de prelucrare a datelor cu caracter personal a O.C.N. „IuteCredit” S.R.L., disponibilă la adresa: <https://iute.md/politica-de-confidentialitate/>.

48. Pentru asigurarea funcționalităților Sistemului MyIute, Compania recurge la prestatorii de servicii menționați la pct. 35A. Acești prestatori prelucrează datele cu caracter personal în baza unui contract încheiat cu Compania și exclusiv în conformitate cu instrucțiunile acesteia, cu excepția cazului în care aceștia acționează în calitate de operatori independenți, situație în care prelucrarea este supusă și condițiilor propriilor politici de confidențialitate.

48A. În cadrul procesului de onboarding și al aplicării măsurilor continue de precauție privind clienții, Compania efectuează prelucrări automatizate, inclusiv crearea de profiluri, în scopul verificării identității, al stabilirii nivelului de risc, al screeningului Clientului și, în cazul depunerii unei cereri de produs, al evaluării bonității. Aceste prelucrări sunt necesare pentru încheierea și executarea contractului și pentru respectarea obligațiilor legale ale Companiei, în timp ce prelucrarea datelor biometrice se efectuează în baza consimțământului explicit al Clientului, exprimat înainte de începerea procesului de identificare. În cazul în care o decizie este luată exclusiv prin mijloace automatizate și produce efecte juridice în privința Clientului, acesta are dreptul de a obține intervenția umană din partea Companiei, de a-și exprima punctul de vedere și de a contesta decizia, adresându-se în scris la adresa dpo@iute.md.



49. Subiectul datelor cu caracter personal beneficiază de următoarele drepturi: dreptul de acces, dreptul de a fi informat, dreptul la rectificare, dreptul la ștergerea datelor, dreptul la restricționarea prelucrării, dreptul la opoziție, dreptul la portabilitatea datelor, dreptul de a-și retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate anterior retragerii, dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automatizată, precum și dreptul de a depune o plângere la Centrul Național pentru Protecția Datelor cu Caracter Personal. Subiectul datelor își poate exercita aceste drepturi adresându-se în scris la următoarea adresă de poștă electronică: dpo@iute.md. Cererile se examinează în termen de o lună de la recepționare, termen care poate fi prelungit cu două luni în cazul în care complexitatea sau numărul cererilor o impune.

VIII. DREPTURILE DE PROPRIETATE INTELECTUALĂ:

50. Întregul conținut al Sistemului MyIute – imagini, texte, elemente grafice, simboluri, scripturi, programe și alte date – este proprietatea Companiei și a furnizorilor săi și este protejat de legislația privind dreptul de autor și de legile privind proprietatea intelectuală și industrială. Utilizarea, fără acordul Companiei, a oricăruia dintre elementele enumerate mai sus se sancționează în conformitate cu legislația în vigoare.

IX. JUSTIFICAREA PRIN IMPEDIMENT:

51. Compania nu răspunde față de Utilizator pentru neexecutarea oricăror obligații justificată de un impediment/eveniment de forță majoră independent de voința sa, nici pentru funcționarea și conectarea altor rețele naționale sau străine ori pentru activitățile și acțiunile acestora în general. Un impediment independent de voința sa/caz de forță majoră poate include, cu titlu de exemplu, dar fără a se limita la: starea de război (declarată sau nu), conflictul armat, revoluția, insurecția, acțiunile sau amenințările militare ori teroriste, sabotajul, tulburările civile, grevele sau alte acțiuni revendicative, legile, reglementările, deciziile sau directivele, calamitățile naturale, cutremurul, incendiul, explozia, perturbațiile solare sau meteorologice, situațiile de urgență publică ori orice altă împrejurare independentă de voința sa. Compania va lua toate măsurile necesare pentru a asigura disponibilitatea maximă a aplicației în cazul impedimentelor independente de voința sa și în cazurile de forță majoră, adică al evenimentelor independente de voința sa.

X. ÎNCETAREA UTILIZĂRII MYIUTE:

52. Încetarea utilizării Sistemului MyIute de către Utilizator poate interveni în următoarele situații:

a) la inițiativa Utilizatorului, prin dezinstalarea Sistemului de pe dispozitivul său sau prin solicitarea blocării accesului; dezinstalarea aplicației nu duce la încetarea relației de afaceri, a contractelor încheiate sau a obligațiilor ce decurg din acestea;

b) la inițiativa Companiei, în cazul încălcării de către Utilizator a prevederilor prezenților Termeni MyIute;

c) la încetarea relației de afaceri dintre Client și Companie;

d) în cazul în care Clientului i se atribuie statutul de risc neacceptat sau de Client inclus în lista neagră, în conformitate cu pct. 34A.

XI. PENTRU CE NU PURTĂM RĂSPUNDERE:

53. Punem la dispoziție Sistemul MyIute exclusiv pentru uz personal. Nu toate serviciile Sistemului MyIute vor funcționa pe toate echipamentele mobile.

54. Acceptați că Sistemul nu va fi furnizat fără erori sau în mod neîntrerupt și că anumite imperfecțiuni nu vor fi remediate în momentul apariției lor.

XII. DISPOZIȚII FINALE:

55. Compania poate suspenda sau modifica imediat Sistemul MyIute, pentru orice motiv, inclusiv în cazul în care sunt necesare lucrări de reparație sau de mentenanță. Putem adăuga periodic funcționalități noi și nu avem obligația de a asigura vreo funcționalitate anume prin MyIute. Putem retrage MyIute, însă, într-un astfel de caz, vă vom notifica cu cel puțin 30 de zile în avans.

56. În cazul în care în cadrul Sistemului MyIute sunt implementate și puse la dispoziție servicii suplimentare, acestea se supun aceluiași reguli și condiții cuprinse în prezentele clauze, cu excepția cazului în care fac obiectul unor condiții separate.

57. Orice neînțelegeri și/sau litigii apărute între Client și Companie în baza utilizării Sistemului MyIute se soluționează pe cale amiabilă, prin negocieri între părți. În cazul epuizării tuturor mijloacelor de soluționare amiabilă a litigiilor, acestea se soluționează de instanțele de judecată competente, în conformitate cu legislația Republicii Moldova.

XIII. DATE DE CONTACT:

58. Dacă aveți întrebări sau neclarități referitoare la Termenii MyIute, vă rugăm să ne contactați la:

- **E-mail:** info@iute.md;
- **Telefon:** +373 22 801 500;
- **Adresă:** mun. Chișinău, bd. Ștefan cel Mare și Sfânt 182, etajul 5, Republica

Moldova.

