

POLITICA

privind protecția datelor cu caracter personal

a Organizației de Creditare Nebancară „CAPITAL LEASING” SRL

IDNO: 0982104031985

Sediul: mun. Chișinău, Republica Moldova, str. Calea Ieșilor, 10

Versiunea 1.0

Data intrării în vigoare: 23 august 2026

mun. Chișinău, 2026

SECȚIUNEA 1. DISPOZIȚII GENERALE.

1.1. Prezenta Politică privind protecția datelor cu caracter personal (în continuare — „Politica”) a fost elaborată de Organizația de Creditare Nebancară „CAPITAL LEASING” SRL (în continuare — „Societatea”, „Operatorul”, „Compania”) în scopul asigurării protecției drepturilor și libertăților persoanelor fizice la prelucrarea datelor lor cu caracter personal și în conformitate cu următoarele acte normative ale Republicii Moldova (în continuare — „RM”):

- Legea nr. 195 din 25.07.2024 privind protecția datelor cu caracter personal (în continuare — „Legea nr. 195/2024”);
- Legea nr. 1 din 16.03.2018 cu privire la organizațiile de creditare nebancară, care reglementează activitatea Societății de acordare a împrumuturilor și de leasing financiar/operațional;
- Legea nr. 92 din 07.04.2022 privind activitatea de asigurare sau de reasigurare, aplicabilă intermedierei în asigurări, în partea ce ține de activitatea de bancassurance desfășurată de Societate;
- Legea nr. 308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului (în continuare — „Legea nr. 308/2017”);
- Legea nr. 122 din 29.05.2008 privind birourile istoriilor de credit;
- Legea nr. 1543 din 25.02.1998 cu privire la cadastrul bunurilor imobile;
- Legea nr. 880 din 22.01.1992 cu privire la Fondul Arhivistic al Republicii Moldova;
- Legea nr. 105 din 13.03.2003 privind protecția consumatorilor;
- Legea nr. 284 din 22.07.2004 privind serviciile societății informaționale;
- Codul muncii și Codul civil al RM,;
- alte acte normative aplicabile ale RM, inclusiv practica de aplicare a Regulamentului (UE) 2016/679 (GDPR), pe ale cărui principii se bazează Legea nr. 195/2024, și practica altor organizații financiare din Moldova și din străinătate.

1.2. Politica stabilește: scopurile și principiile prelucrării datelor cu caracter personal de către Societate; categoriile de persoane vizate și categoriile de date cu

caracter personal prelucrate; temeiurile juridice și termenele de prelucrare și păstrare a datelor; măsurile organizatorice și tehnice de asigurare a securității acestora; drepturile persoanelor vizate și modul de exercitare a acestora; modul de examinare a sesizărilor și reclamațiilor; modul de interacțiune cu persoanele împuternicite de operator și cu registrele de stat; răspunderea pentru încălcarea cerințelor legislației privind protecția datelor cu caracter personal.

1.3. Prezenta Politică se aplică tuturor subdiviziunilor structurale ale Societății, tuturor angajaților acesteia, indiferent de funcția deținută și de tipul contractului încheiat (contract individual de muncă, contract civil, cumul de funcții), inclusiv angajaților care nu au un loc de muncă fix, precum și tuturor terților (persoane împuternicite, contractanți, parteneri) cărora Societatea le încredințează prelucrarea datelor cu caracter personal sau care obțin acces la date cu caracter personal în legătură cu executarea obligațiilor contractuale față de Societate.

1.4. Prezenta Politică urmează a fi plasată în acces liber pe site-ul oficial al Societății și adusă la cunoștința fiecărui angajat care are acces la date cu caracter personal, sub semnătură — la angajare și la fiecare modificare a Politicii.

1.5. Societatea, fiind o organizație de creditare nebancară, desfășoară următoarele tipuri de activitate legate de prelucrarea datelor cu caracter personal: (a) leasing financiar; (b) leasing operațional; (c) acordarea de împrumuturi persoanelor fizice și juridice; (d) activitate de intermediere în asigurări (bancassurance). Particularitățile prelucrării datelor cu caracter personal pentru fiecare dintre aceste tipuri de activitate sunt stabilite în Secțiunea 12 din prezenta Politică.

1.6. Societatea conștientizează și recunoaște răspunderea sa în calitate de operator de date cu caracter personal, care prelucrează volume semnificative de informații financiare, de identificare și, în anumite cazuri, biometrice, și se angajează să aplice standarde sporite de protecție a datelor cu caracter personal, comparabile cu standardele aplicate de cele mai mari organizații financiare din Republica Moldova și din străinătate.

SECȚIUNEA 2. TERMENI ȘI DEFINIȚII.

Termen	Definiție
Date cu caracter personal	Orice informație referitoare la o persoană fizică identificată sau identificabilă (persoana vizată); este identificabilă persoana care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi numele, un număr de identificare (IDNP), date de localizare, un identificator online, sau la unul ori mai multe elemente specifice identității fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.
Categorii speciale de date cu caracter personal	Date care dezvăluie originea rasială sau etnică, opiniile politice, convingerile religioase sau filosofice, apartenența sindicală, precum și date genetice, date biometrice pentru identificarea unică a unei persoane fizice, date privind starea de sănătate sau viața ori orientarea sexuală.
Date biometrice	Date cu caracter personal obținute în urma unui tratament tehnic specific, referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice (inclusiv date dactiloscopice — amprente digitale), care permit identificarea unică a acestei persoane.
Prelucrarea datelor cu caracter personal	Orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate: colectare, înregistrare, organizare, structurare, stocare, adaptare, extragere, utilizare, divulgare prin transmitere, diseminare sau punere la dispoziție în orice alt mod, alăturare, restricționare, ștergere sau distrugere.
Operatorul (Societatea)	Organizația de creditare nebancaară „CAPITAL LEASING” SRL, care stabilește, singură sau împreună cu alții, scopurile și mijloacele de prelucrare a datelor cu caracter personal.
Persoana împuternicită de operator	Persoana fizică sau juridică ce prelucrează date cu caracter personal în numele Societății, în baza unui contract scris (în special, compania DSI, care administrează sistemul informațional al Societății).
Persoana vizată	Persoana fizică identificată sau identificabilă ale cărei date cu caracter personal sunt prelucrate de Societate (client, garant, angajat, candidat la angajare, reprezentant al contractantului, vizitator al oficiului, utilizator al site-ului).
Consimțământul persoanei vizate	Orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate, prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate.
Pseudonimizare	Prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anumite persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică.
Încălcarea securității datelor cu caracter personal (incident/breșă)	O încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate în alt mod, sau la accesul neautorizat la acestea.
Transfer transfrontalier de date	Transferul de date cu caracter personal de către un operator sau o persoană împuternicită aflată pe teritoriul RM către un destinatar situat în afara teritoriului RM.
Responsabilul cu protecția datelor cu caracter personal (Data Protection Officer, DPO)	Persoana desemnată de Societate (sau contractată în bază de contract) pentru monitorizarea respectării cerințelor legislației privind protecția datelor cu caracter personal, consilierea Societății și a angajaților, precum și pentru interacțiunea cu Centrul Național pentru Protecția Datelor și cu persoanele vizate.

Crearea de profiluri	Orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea acestor date pentru a evalua anumite aspecte personale ale unei persoane fizice, în special pentru a analiza sau prognoza aspecte privind capacitatea de plată, situația economică, comportamentul.
----------------------	---

SECȚIUNEA 3. PRINCIPIILE PRELUCRĂRII DATELOR CU CARACTER PERSONAL.

3.1. În conformitate cu art. 5 din Legea nr. 195/2024, la prelucrarea datelor cu caracter personal Societatea se conduce după următoarele principii și poartă răspundere pentru respectarea acestora și pentru posibilitatea de a demonstra o astfel de respectare (principiul responsabilității):

a) Legalitate, echitate și transparență — datele cu caracter personal sunt prelucrate în mod legal, echitabil și transparent față de persoana vizată; persoana vizată este informată despre faptele și scopurile prelucrării într-o formă clară și accesibilă.

b) Limitarea legată de scop — datele sunt colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri.

c) Reducerea la minimum a datelor — volumul și natura datelor prelucrate trebuie să fie adecvate, relevante și limitate la ceea ce este necesar pentru scopurile prelucrării; Societatea nu colectează date „de rezervă”.

d) Exactitate — datele trebuie să fie exacte și, dacă este necesar, actualizate; Societatea ia toate măsurile rezonabile pentru a se asigura că datele inexacte sunt șterse sau rectificate fără întârziere.

e) Limitarea legată de stocare — datele sunt păstrate într-o formă care permite identificarea persoanei vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor prelucrării, cu excepția arhivării în interes public, cercetării științifice sau istorice ori în scopuri statistice.

f) Integritate și confidențialitate — datele sunt prelucrate într-un mod care asigură securitatea adecvată, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, distrugerii sau deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare.

g) Responsabilitate — Societatea răspunde de respectarea principiilor menționate mai sus și trebuie să poată demonstra această respectare la prima cerere a Centrului Național, inclusiv prin ținerea Registrului operațiunilor de prelucrare a datelor cu caracter personal, a politicilor interne și a evidenței consimțămintelor.

SECȚIUNEA 4. CATEGORII DE PERSOANE VIZATE.

4.1. Societatea prelucrează date cu caracter personal ale următoarelor categorii de persoane vizate:

- clienți — persoane fizice (beneficiari de împrumuturi, locatari în cadrul contractelor de leasing, asigurați în baza contractelor încheiate prin intermedierea Societății);
- reprezentanți, conducători, beneficiari efectivi și persoane de contact ale clienților — persoane juridice;
- garanți, cobeneficiari de împrumut, debitori gajiști și alte persoane implicate în garantarea obligațiilor din contractele de împrumut/leasing;
- angajații Societății și persoanele care activează în baza unor contracte civile;
- candidați la angajare în cadrul Societății;
- reprezentanți ai contractanților, furnizorilor și partenerilor Societății (inclusiv ai saloanelor auto, ai companiilor de asigurări partenere, ai companiei DSI);
- vizitatori ai oficiului Societății (în volumul de date obținut prin sistemele de videosupraveghere și control al accesului);
- utilizatori ai site-ului oficial al Societății.

SECȚIUNEA 5. CATEGORIILE DE DATE CU CARACTER PERSONAL PRELUCRATE.

5.1. Categorii generale de date cu caracter personal.

Societatea prelucrează, în special, următoarele date: numele, prenumele, patronimicul; numărul de identificare personal (IDNP); datele actului de identitate (seria, numărul, data și organul emitent, termenul de valabilitate); data și locul nașterii; cetățenia; adresa domiciliului și/sau reședinței; date de contact (numărul de telefon, adresa de e-mail); date privind starea civilă și componența familiei (în volumul necesar evaluării capacității de plată); date privind veniturile, locul de

muncă, funcția și vechimea în muncă; date privind rechizitele bancare și operațiunile de plată; date din istoricul de credit; date privind bunurile mobile și imobile care fac obiectul leasingului sau gajului; imaginea fotografică (inclusiv cea obținută prin sistemele de videosupraveghere); date conținute în corespondența și sesizările persoanelor vizate.

5.2. Categoriile speciale de date cu caracter personal (date biometrice).

La oficiul Societății, unele accese sunt dotate cu încuietoare cu cititor dactiloscopic. Datele biometrice ale angajaților Societății sunt prelucrate exclusiv în scopul controlului accesului fizic în incintele Societății și exclusiv în baza consimțământului scris liber exprimat, specific, informat și lipsit de ambiguitate al fiecărui angajat, obținut de Societate în prealabil. Modul și condițiile unei astfel de prelucrări sunt stabilite detaliat de prezenta Politică.

5.3. Societatea nu colectează și nu prelucrează date privind originea rasială sau etnică, opiniile politice, convingerile religioase sau filosofice, apartenența sindicală, date genetice, date privind starea de sănătate, viața sau orientarea sexuală a persoanelor vizate, cu excepția cazurilor în care prelucrarea anumitor astfel de date este expres prevăzută de legislație sau este necesară în cadrul prestării serviciilor de bancassurance (de exemplu, la intermedierea încheierii unui contract de asigurare de viață sau de sănătate) și se realizează exclusiv cu consimțământul explicit al persoanei vizate și în volumul stabilit de cerințele asigurătorului partener.

SECȚIUNEA 6. SCOPURILE ȘI TEMEIURILE JURIDICE ALE PRELUCRĂRII DATELOR CU CARACTER PERSONAL.

6.1. Prelucrarea datelor cu caracter personal se realizează de Societate numai în prezența a cel puțin unuia dintre temeiurile juridice prevăzute la art. 6 din Legea nr. 195/2024:

- consimțământul persoanei vizate;
- necesitatea executării unui contract la care persoana vizată este parte sau efectuarea de demersuri la cererea acesteia înainte de încheierea unui contract;
- necesitatea îndeplinirii unei obligații legale care revine Societății;
- necesitatea protejării intereselor vitale ale persoanei vizate;

- necesitatea îndeplinirii unei sarcini de interes public;
- necesitatea prelucrării în scopul intereselor legitime urmărite de Societate sau de o parte terță, cu excepția cazului în care aceste interese sunt anulate de interesele sau drepturile și libertățile fundamentale ale persoanei vizate.

Direcția de activitate / proces	Scopul prelucrării	Temeiul juridic
Leasing financiar și operațional	Încheierea și executarea contractului de leasing, evaluarea obiectului leasingului și a capacității de plată a clientului	Executarea contractului / demersuri precontractuale la cererea persoanei vizate; obligație legală (creditare responsabilă)
Acordarea de împrumuturi persoanelor fizice și juridice	Evaluarea capacității de plată, adoptarea deciziei de finanțare, încheierea și executarea contractului de împrumut, recuperarea datoriei	Executarea contractului; obligație legală (creditare responsabilă); interesul legitim al Societății
Bancassurance (intermediere în asigurări)	Selectarea și perfectarea contractului de asigurare prin intermediul partenerului-asigurător	Consimțământul persoanei vizate; executarea contractului de mandat/agenție
Identificarea clientului (KYC/AML)	Stabilirea identității, a beneficiarului efectiv, a sursei mijloacelor bănești	Obligație legală conform Legii nr. 308/2017 privind PSB/FT
Interacțiunea cu Biroul istoriilor de credit	Formarea și obținerea istoricului de credit pentru evaluarea capacității de plată	Consimțământul persoanei vizate / obligație legală conform Legii nr. 122/2008
Interacțiunea cu Cadastrul	Verificarea statutului juridic al obiectului gajului/leasingului	Interesul legitim al Societății / obligație legală
Administrarea resurselor umane (HR)	Încheierea și executarea contractului individual de muncă, calcularea salariului, asigurarea socială și medicală	Obligație legală; executarea contractului
Videosupraveghere la oficiu	Asigurarea securității bunurilor, angajaților și vizitatorilor, prevenirea și investigarea contravențiilor/infracțiunilor	Interesul legitim al Societății
Control biometric al accesului	Controlul accesului în incintele cu acces limitat	Consimțământul angajatului
Marketing direct (la dorința clientului)	Informarea despre produsele și serviciile Societății	Consimțământul persoanei vizate (revocabil în orice moment)
Examinarea sesizărilor și reclamațiilor	Recepționarea, înregistrarea și examinarea sesizărilor persoanelor vizate, protejarea drepturilor Societății	Obligație legală; interes legitim

6.2. Prelucrarea categoriilor speciale de date (în special, a datelor biometrice ale angajaților) este permisă numai în prezența unui consimțământ scris explicit al

persoanei vizate sau a unui alt temei expres prevăzut de legislație, cu respectarea măsurilor suplimentare de protecție prevăzute de prezenta Politică.

SECȚIUNEA 7. SURSELE ȘI MODUL DE COLECTARE A DATELOR CU CARACTER PERSONAL.

7.1. Ca regulă generală, datele cu caracter personal sunt colectate de Societate direct de la persoana vizată — la adresarea personală la oficiu, la încheierea contractului la partener (salon auto).

7.2. În cazurile prevăzute de legislație și în volumul necesar scopurilor indicate în Secțiunea 6, Societatea este în drept să obțină date din alte surse: ***de la Biroul istoriilor de credit*** — informații privind istoricul de credit al persoanei vizate (cu consimțământul acesteia sau în baza unui alt temei legal); ***de la Cadastrul bunurilor imobile*** — informații privind statutul juridic al bunului care face obiectul tranzacției; ***de la contractanți-parteneri*** (în special, de la saloanele auto, la încheierea tranzacțiilor de leasing) — date transmise cu consimțământul persoanei vizate în scopul încheierii contractului; ***din surse publice și registre publice*** — în volumul necesar verificării veridicității datelor furnizate și în scopurile PSB/FT.

7.3. Societatea colectează date cu caracter personal în volumul minim necesar, suficient pentru atingerea scopului declarat, și nu colectează date care nu au legătură cu scopul unei operațiuni concrete de prelucrare. La completarea formularelor (inclusiv pe site) câmpurile care nu sunt strict necesare sunt marcate ca opționale.

SECȚIUNEA 8. TERMENELE DE PĂSTRARE A DATELOR CU CARACTER PERSONAL.

8.1. În conformitate cu principiul limitării legate de stocare (art. 5 din Legea nr. 195/2024), datele cu caracter personal sunt păstrate de Societate într-o formă care permite identificarea persoanei vizate pe o perioadă care nu depășește perioada necesară scopurilor pentru care sunt prelucrate, ținând cont de termenele stabilite de legislația specială (în special, Legea nr. 308/2017 privind PSB/FT și Legea nr. 880/1992 cu privire la Fondul Arhivistic).

Categoria de date / documente	Termenul de păstrare	Temei / acțiuni ulterioare
Dosarul clientului (documente de identificare, contract, documente de plată, corespondența privind tranzacția)	minimum 5 ani de la încetarea raporturilor contractuale	art. 5 din Legea nr. 195/2024, Legea nr. 308/2017 (PSB/FT); la expirarea termenului — distrugere pe bază de proces-verbal sau transmitere în arhivă conform nomenclatorului dosarelor
Datele persoanelor cărora li s-a refuzat finanțarea („refuzați”)	până la 1 an de la data refuzului	Interesul legitim al Societății (apărarea împotriva reclamațiilor, statistică, prevenirea fraudei); ulterior — anonimizare sau distrugere
Înregistrările sistemelor de videosupraveghere	până la 30 de zile calendaristice	Suprascrisiere/ștergere automată; prelungire — doar pentru fragmentul concret solicitat în cadrul unei investigații sau proceduri judiciare
Registrul accesărilor sistemului biometric (intrări/ieșiri)	Ștergere imediată la încetarea oficială a raporturilor de muncă	Regulament intern de securitate a informației; șablonul biometric se șterge în ziua concedierii angajatului
Dosarele personale și documentele angajaților (de personal, de calcul)	pe durata raporturilor de muncă și ulterior conform nomenclatorului dosarelor Societății, aprobat ținând cont de Legea nr. 880/1992 (pentru anumite categorii de documente de calcul — termene de păstrare îndelungate -75 de ani)	Codul muncii al RM, Legea nr. 880/1992 cu privire la Fondul Arhivistic
CV-urile și datele candidaților care nu au fost angajați	6–12 luni sau până la revocarea consimțământului	Consimțământul persoanei vizate; ulterior — ștergere, dacă candidatul nu și-a exprimat acordul pentru o păstrare mai îndelungată în vederea unor viitoare posturi vacante
Sesizări, reclamații și corespondența cu persoanele vizate/registrele de evidență	minimum 3 ani de la data înregistrării sesizării/5 ani	Principiul responsabilității (art. 5 din Legea nr. 195/2024); posibilitatea verificării de către Centrul Național
Date pentru scopuri de marketing direct	până la revocarea consimțământului persoanei vizate, cu revizuirea anuală a actualității consimțământului sau max. 2 ani de la ultima interacțiune comercială activă.	Consimțământul persoanei vizate
Evidența consimțămintelor persoanelor vizate	întreaga perioadă de prelucrare + 3 ani de la încetarea acesteia	Confirmarea legalității prelucrării (principiul responsabilității)

8.2. La expirarea termenelor de păstrare stabilite, datele cu caracter personal urmează a fi distruse iremediabil (pentru documentele pe suport de hârtie — prin mărunțire, cu întocmirea unui proces-verbal de distrugere; pentru datele în formă electronică — prin ștergere iremediabilă prin mijloace care exclud recuperarea) sau anonimizate, ori, dacă documentul este atribuit conform nomenclatorului aprobat

unor dosare cu termen de păstrare îndelungat sau permanent, — transmise în arhiva Societății, în modul stabilit la pct. 11.8 din prezenta Politică.

8.3. Prelungirea termenului de păstrare a datelor peste cel indicat în prezenta Secțiune este permisă exclusiv în cazurile în care acest lucru este necesar pentru constatarea, exercitarea sau apărarea unor pretenții legale ale Societății ori pentru executarea unei cereri a unui organ de stat competent, — pe perioada necesară scopului respectiv, cu documentarea motivelor unei asemenea prelungiri.

SECȚIUNEA 9. DREPTURILE PERSOANELOR VIZATE ȘI MODUL DE EXERCITARE A ACESTORA.

9.1. Fiecare persoană vizată ale cărei date sunt prelucrate de Societate beneficiază de următoarele drepturi:

Dreptul	Conținutul	Termenul de exercitare
La informare	De a obține, într-o formă clară, informații privind scopurile, temeiurile juridice, categoriile de date prelucrate, destinatarii, termenele de păstrare și drepturile sale — la colectarea datelor sau la cerere	La momentul colectării datelor / fără întârziere
De acces	De a obține confirmarea faptului prelucrării și o copie a datelor sale cu caracter personal	1 lună
La rectificare	De a solicita rectificarea datelor inexacte sau completarea datelor incomplete	1 lună
La ștergerea datelor („dreptul de a fi uitat”)	De a solicita ștergerea datelor în cazul dispariției scopului prelucrării, al revocării consimțământului sau al ilegalității prelucrării, cu excepția cazurilor în care păstrarea este necesară pentru îndeplinirea unei obligații legale	1 lună
La restricționarea prelucrării	De a solicita suspendarea temporară a prelucrării în cazurile prevăzute de lege (de exemplu, în perioada verificării exactității datelor)	1 lună
La portabilitatea datelor	De a primi datele furnizate Societății într-un format structurat, prelucrabil automat și de a le transmite altui operator	1 lună
La opoziție	De a se opune prelucrării efectuate în baza interesului legitim, precum și, necondiționat, prelucrării în scopuri de marketing direct	Fără întârziere pentru marketing; 1 lună — celelalte cazuri
La refuzul deciziilor automatizate	De a nu face obiectul unei decizii bazate exclusiv pe prelucrare automată (inclusiv crearea de profiluri) care produce efecte juridice, fără dreptul la intervenție umană	1 lună
La revocarea consimțământului	De a revoca în orice moment consimțământul dat anterior, la fel de simplu cum a fost acordat, fără a afecta legalitatea prelucrării efectuate până la revocare	Fără întârziere
La depunerea unei plângeri	De a se adresa cu o plângere Centrului Național pentru Protecția Datelor cu Caracter Personal al RM și/sau instanței de judecată	În orice moment

9.2. Cererea privind exercitarea drepturilor se depune de persoana vizată în formă scrisă — pe suport de hârtie la sediul Societății, prin e-mail la adresa Responsabilului cu protecția datelor cu caracter personal sau prin formularul de pe site-ul oficial al Societății. Cererea trebuie să conțină informații suficiente pentru identificarea solicitantului ca persoană vizată a datelor respective; Societatea este în drept să solicite o confirmare suplimentară a identității solicitantului în cazul unor îndoieli întemeiate, dar nu este în drept să solicite date excesive în raport cu scopurile unei asemenea identificări (*model de cerere găsiți pe site*).

9.3. Răspunsul la cerere este furnizat de Societate gratuit, în termen de cel mult o lună de la data primirii cererii. Acest termen poate fi prelungit cu încă două luni, ținând cont de complexitatea și numărul cererilor, Societatea informând persoana vizată despre prelungirea termenului și despre motivele întârzierii în cursul primei luni. În cazul unei cereri vădit neîntemeiate sau excesive (în special, în caz de repetare), Societatea este în drept să perceapă o taxă rezonabilă, ținând cont de costurile administrative, sau să refuze satisfacerea cererii, motivând un asemenea refuz. Toate datele referitoare la examinarea cererilor se înscriu în Registrul de specialitate.

9.4. Modul de întocmire a sesizărilor (reclamațiilor) și cerințele privind conținutul corespondenței aferente sunt stabilite detaliat în Secțiunea 16 din prezenta Politică.

SECȚIUNEA 10. RESPONSABILUL CU PROTECȚIA DATELOR CU CARACTER PERSONAL. OBLIGAȚIILE OPERATORULUI.

10.1. Ținând cont de faptul că Societatea prelucrează, pe o bază sistematică și într-un volum semnificativ, date cu caracter personal ale clienților de servicii financiare, efectuează o monitorizare sistematică a zonelor publice (videosupraveghere) și prelucrează, de asemenea, categorii speciale de date (date biometrice ale angajaților), Societatea desemnează un Responsabil cu protecția datelor cu caracter personal (DPO) dintre angajații care dețin studii superioare și calificarea corespunzătoare, sau contractează o astfel de persoană în bază contractuală (externalizare).

10.2. Funcțiile Responsabilului cu protecția datelor cu caracter personal includ:

a) informarea și consilierea operatorului sau a persoanei împuternicite de operator, precum și a angajaților care se ocupă de prelucrare, cu privire la obligațiile care le revin în temeiul prezentei legi și al altor acte normative referitoare la protecția datelor;

b) monitorizarea respectării prezentei legi și a altor acte normative referitoare la protecția datelor, precum și a politicilor operatorului sau ale persoanei împuternicite de operator în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;

c) furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia, în conformitate cu art. 35;

d) cooperarea cu Centrul;

e) asumarea rolului de punct de contact pentru Centru cu privire la aspectele legate de prelucrare, inclusiv consultarea prealabilă prevăzută la art. 36, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune;

f) recepționarea și coordonarea examinării sesizărilor persoanelor vizate, , inclusiv la notificarea încălcărilor de securitate;

g) ținerea Registrului operațiunilor de prelucrare a datelor cu caracter personal și a Registrului de evidență a incidentelor

10.3. În îndeplinirea sarcinilor sale, responsabilul cu protecția datelor ține cont în mod corespunzător de riscul asociat operațiunilor de prelucrare, luând în considerare natura, domeniul de aplicare, contextul și scopurile prelucrării.

10.4. Datele de contact ale Responsabilului (Responsabilului cu protecția datelor cu caracter personal) se publică pe site-ul oficial al Societății și se indică în ordinele și fișele de post corespunzătoare.

10.5. Societatea, în calitate de Operator de date cu caracter personal, este obligată, în special:

- să țină Registrul operațiunilor de prelucrare a datelor cu caracter personal, care conține informații privind scopurile, categoriile de persoane vizate și de date, destinatarii, termenele de păstrare și măsurile de securitate aplicate pentru fiecare operațiune de prelucrare;
- să efectueze Evaluarea impactului asupra protecției datelor (DPIA) înainte de începerea prelucrării care poate genera un risc ridicat pentru drepturile și libertățile persoanelor vizate (în special, videosupravegherea, controlul biometric al accesului, scoring-ul automatizat);
- să asigure protecția datelor „începând cu momentul conceperii și în mod implicit” la implementarea unor procese și sisteme informaționale noi;
- să încheie contracte scrise privind prelucrarea datelor cu caracter personal cu toate persoanele împuternicite (inclusiv cu DSI) și cu alți terți care obțin acces la date cu caracter personal;
- să notifice Centrul Național pentru Protecția Datelor cu Caracter Personal despre încălcarea securității datelor cu caracter personal în cel mult 72 de ore de la momentul în care Societatea a luat cunoștință de încălcare, dacă aceasta poate genera un risc pentru drepturile și libertățile persoanelor vizate, precum și să informeze persoanele vizate afectate, fără întârzieri nejustificate, dacă riscul este ridicat;
- să țină Registrul de evidență a incidentelor, indiferent de faptul notificării Centrului Național;
- să asigure instruirea periodică (cel puțin o dată pe an) a angajaților și verificarea eficienței măsurilor de protecție aplicate.

SECȚIUNEA 11. MĂSURI ORGANIZATORICE ȘI TEHNICE DE ASIGURARE A SECURITĂȚII DATELOR CU CARACTER PERSONAL.

11.1. În conformitate cu art. 32 din Legea nr. 195/2024, Societatea este obligată să implementeze măsuri tehnice și organizatorice adecvate nivelului tehnologic, costurilor de implementare, naturii, volumului, contextului și scopurilor prelucrării, precum și riscurilor pentru drepturile și libertățile persoanelor vizate, pentru a asigura un nivel de securitate corespunzător al datelor cu caracter personal,

inclusiv, după caz: pseudonimizarea și criptarea datelor; asigurarea confidențialității, integrității, disponibilității și rezilienței permanente a sistemelor și serviciilor de prelucrare; capacitatea de a restabili în timp util disponibilitatea datelor în caz de incident fizic sau tehnic; o procedură de testare și evaluare periodică a eficacității măsurilor de securitate. În continuare sunt prezentate măsurile concrete aplicate de Societate, ținând cont de specificul activității și structurii sale.

11.2. Managementul personalului și delimitarea accesului.

Accesul la datele cu caracter personal se acordă angajaților Societății exclusiv în baza principiului „necesității de a cunoaște”, în volumul strict necesar îndeplinirii atribuțiilor de serviciu, și se documentează conform matricei de acces aprobate de directorul Societății.

Toți cei 20 (douăzeci) de angajați ai Societății care au acces la date cu caracter personal urmează instruirea introductivă privind protecția datelor cu caracter personal la angajare și instruirea periodică cel puțin o dată pe an; cu fiecare angajat se încheie un angajament scris de confidențialitate, care face parte integrantă din contractul individual de muncă sau este un acord separat. Angajatul ia cunoștință, sub semnătură, de prezenta Politică și de instrucțiunile interne privind securitatea informației.

Instruirea periodică se realizează cel puțin o dată pe an pentru toți angajații, iar pentru personalul cu acces la categorii specifice de date sau care activează în teren/saloane partenere se organizează sesiuni practice adaptate riscurilor specifice activității lor.

Accesul angajatului la sistemele informaționale, la incinte și la sistemul biometric se blochează cel târziu în ziua încetării raporturilor de muncă (conturile de utilizator se blochează, ecusoanele și șabloanele biometrice se șterg).

11.3. Sistemele informaționale. Interacțiunea cu administratorul sistemului informațional (DSI)

Evidența și prelucrarea electronică a datelor cu caracter personal se realizează în sistemul informațional administrat de organizația contractată DSI, care, în raport

cu Societatea, are calitatea de Persoană împuternicită de operator în sensul Legii nr. 195/2024.

Cu persoana împuternicită (DSI) este încheiat un Contract scris privind prelucrarea datelor cu caracter personal, care trebuie să conțină cel puțin: obiectul, natura, durata și scopul prelucrării, categoriile de date cu caracter personal și de persoane vizate; obligația DSI de a prelucra datele exclusiv conform instrucțiunilor documentate ale Societății; angajamentul de confidențialitate, aplicabil întregului personal al DSI care are acces la date; obligația DSI de a asigura măsuri de securitate echivalente cerințelor art. 32 din Legea nr. 195/2024; interdicția de a angaja subîmputerniciți fără acordul scris prealabil al Societății; obligația DSI de a sprijini Societatea în exercitarea drepturilor persoanelor vizate și în notificarea încălcărilor de securitate; modul de restituire sau distrugere a datelor la finalizarea prestării serviciilor; dreptul Societății de a efectua verificări (audit) privind respectarea condițiilor contractului.

Societatea efectuează o evaluare periodică, cel puțin o dată pe an, a conformității DSI cu cerințele legislației privind protecția datelor cu caracter personal și cu condițiile contractului încheiat, inclusiv verificarea măsurilor tehnice de protecție aplicate.

11.4. Politica parolelor.

Parola de acces la stațiile de lucru și la sistemele informaționale ale Societății trebuie să conțină minimum 10–12 caractere, inclusiv litere mari și mici din alfabetul latin, cifre și caractere speciale, nu trebuie să coincidă cu nici una dintre ultimele 5 (cinci) parole ale utilizatorului respectiv și nu trebuie să conțină informații personale ușor de dedus (nume, data nașterii etc.).

Periodicitatea recomandată (optimă) de schimbare planificată a parolelor, stabilită de Societate: pentru utilizatorii obișnuiți — cel puțin o dată la 90 (nouăzeci) de zile calendaristice (trimestrial); pentru conturile cu drepturi extinse (administratori de sistem, angajați cu acces la Biroul istoriilor de credit, la Cadastru sau la modulele financiare ale sistemului informațional) — cel puțin o dată la 60 (șaizeci) de zile calendaristice. Indiferent de periodicitatea planificată, schimbarea

neplanificată a parolei este obligatorie și se efectuează fără întârziere: la cea mai mică suspiciune de compromitere a parolei; la concedierea, transferul sau suspendarea temporară a angajatului; în cazul depistării unui incident de securitate la persoana împuternicită (DSI).

Periodicitatea menționată este stabilită de Societate ca un echilibru optim între recomandările actuale privind gestionarea parolelor și riscurile sporite specifice sectorului financiar și accesului la registre de stat sensibile (Biroul istoriilor de credit, Cadastru). În acest sens, ca măsură de protecție prioritară, alături de schimbarea periodică a parolelor, accesul la sistemul de gestiune a leasingului și la e-mailul corporativ este permis exclusiv prin autentificare multifactor (2FA/MFA).

Transmiterea parolelor către terți, precum și păstrarea acestora în formă necriptată sau accesibilă public (notarea pe autocolante de hârtie, păstrarea în fișiere neprotejate) sunt strict interzise și constituie temei pentru răspundere disciplinară.

11.5. Copierea de rezervă și restabilirea datelor.

Copierea de rezervă a bazelor de date ale sistemului informațional este efectuată de DSI în mod regulat (cel puțin o dată pe lună — pentru bazele de date critice, care conțin informații despre clienți și contracte). Copiile de rezervă sunt păstrate în formă criptată, inclusiv pe un amplasament separat fizic (circuit de rezervă), care asigură integritatea datelor în caz de pierdere sau deteriorare a infrastructurii principale. *Testarea procedurii de restabilire a datelor din copiile de rezervă se efectuează cel puțin o dată pe an, cu documentarea rezultatelor.*

11.6. Securitatea fizică a oficiului și videosupravegherea.

Oficiul Societății, situat în mun. Chișinău, este dotat cu un sistem de videosupraveghere, instituit în conformitate cu cerințele legislației privind protecția datelor cu caracter personal.

Videosupravegherea se efectuează exclusiv în scopul asigurării securității bunurilor, angajaților și vizitatorilor Societății, precum și al prevenirii și investigării unor fapte ilegale, și nu este utilizată pentru evidența timpului de muncă, evaluarea performanței profesionale sau alte scopuri incompatibile cu scopul declarat.

Camerele de supraveghere nu sunt instalate în încăperile destinate odihnei personalului și în grupurile sanitare.

Toate zonele aflate sub videosupraveghere sunt marcate cu plăcuțe informative (pictograme), cu indicarea operatorului videosupravegherii și a datelor de contact pentru obținerea de informații suplimentare privind scopurile și condițiile prelucrării — în conformitate cu principiul transparenței.

Termenul de păstrare a înregistrărilor de videosupraveghere este de până la 30 de zile calendaristice, la expirarea căruia înregistrările se șterg automat prin suprascriere ciclică, cu excepția cazurilor în care un fragment concret al înregistrării este solicitat în cadrul investigării unui incident, al unei proceduri disciplinare sau judiciare, ori la cererea legală a unui organ competent, — în acest caz fragmentul respectiv este extras și păstrat separat pe perioada necesară scopurilor menționate, cu consemnarea faptului și a temeiurilor unei asemenea păstrări.

Accesul la înregistrările de videosupraveghere este acordat exclusiv angajaților autorizați (directorul, persoana responsabilă de securitatea informației); fiecare vizionare, extragere sau transmitere a unei înregistrări se consemnează în registrul de evidență a accesului la sistemul de videosupraveghere, cu indicarea datei, orei, persoanei și scopului solicitării și întocmirea procesului-verbal respectiv.

11.7. Sistemul biometric de control al accesului.

Dintre cele două puncte de acces în oficiul Societății, unul se află sub paza unui post de pază fizică, celălalt este dotat cu o încuietoare cu cititor dactiloscopic (biometric).

Întrucât datele dactiloscopice fac parte din categoria specială de date cu caracter personal, prelucrarea acestora se realizează exclusiv în baza consimțământului scris liber exprimat, specific, informat și lipsit de ambiguitate al fiecărui angajat, obținut de Societate înainte de includerea datelor angajatului în sistemul de control al accesului. *(la momentul actual un astfel de consimțământ a fost exprimat de către angajații Societății)*

Angajaților care nu și-au dat consimțământul pentru prelucrarea datelor biometrice sau care ulterior l-au revocat, Societatea le asigură o alternativă de acces

echivalentă (trecerea prin postul de pază sau prin intermediul unui ecuson/card de acces electronic), fără nicio discriminare și fără afectarea drepturilor lor de muncă. Sistemul de control al accesului păstrează nu imaginea grafică a amprenteii digitale, ci șablonul matematic al acesteia, care nu permite restabilirea imaginii biometrice inițiale, fapt considerat de Societate drept o măsură tehnică de minimizare a riscului, în conformitate cu principiul protecției datelor începând cu momentul conceperii. Șablonul biometric al angajatului se șterge cel târziu în ziua concedierii acestuia sau în ziua revocării consimțământului.

11.8. Angajați fără loc de muncă fix (specialiști mobili/în teren).

Angajații Societății care își desfășoară activitatea în afara oficiului (în special, specialiștii care activează în saloane auto și în alte puncte de vânzare, la sediul clientului, fără o legătură strictă cu un anumit loc de muncă) utilizează pentru prelucrarea datelor cu caracter personal exclusiv mijloacele furnizate și configurate de Societate: laptopuri/tablete cu criptare integrală a discului, conexiune VPN securizată la sistemul informațional al Societății, program antivirus actualizat și blocarea automată a ecranului în cazul inactivității ce depășește 5 minute.

Pentru această categorie de angajați sunt stabilite următoarele interdicții: prelucrarea și păstrarea datelor cu caracter personal ale clienților pe dispozitive personale și în spații de stocare în cloud personale; copierea documentelor clienților pe suporturi amovibile fără necesitate de serviciu și fără autorizarea persoanei responsabile; transmiterea și discutarea datelor clientului prin canale de comunicare neprotejate (în special, prin mesagerii personale) și în prezența unor persoane străine.

La lucrul cu documentele clientului (de exemplu, scanarea sau fotografierea actului de identitate) într-un loc necontrolat de Societate (salon auto, alt loc public), angajatul este obligat să se asigure că documentele și ecranul dispozitivului nu sunt accesibile vizual persoanelor străine, iar copiile fizice ale documentelor, dacă sunt create, sunt transmise în aceeași zi lucrătoare la oficiul Societății pentru păstrare în modul stabilit sau sunt distruse, dacă necesitatea lor a dispărut.

11.9. Arhiva.

La expirarea termenelor de utilizare curentă, documentele care conțin date cu caracter personal și care urmează a fi păstrate în continuare, conform nomenclatorului dosarelor aprobat de Societate și Legii nr. 880-XII din 22.01.1992 cu privire la Fondul Arhivistic al Republicii Moldova, sunt transmise în arhiva Societății pe bază de proces-verbal de predare-primire.

Arhiva Societății este amplasată într-o încăpere cu acces limitat (dulapuri/seifuri încuiate, încăpere separată cu control al accesului), protejată împotriva accesului neautorizat, incendiului și inundației. Accesul în arhivă este acordat unui cerc limitat de persoane, conform listei aprobate de directorul Societății; fiecare eliberare a unui dosar din arhivă se consemnează în registrul de evidență, cu indicarea datei, persoanei, scopului consultării și termenului de restituire a documentului.

Documentele cu termenul de păstrare expirat, care nu fac obiectul unei păstrări ulterioare (inclusiv permanente), se distrug în urma expertizei valorii documentelor, cu întocmirea unui proces-verbal de distrugere, aprobat de directorul Societății (de comisia de expertiză, dacă aceasta este constituită).

SECȚIUNEA 12. PARTICULARITĂȚILE PRELUCRĂRII DATELOR CU CARACTER PERSONAL LA DESFĂȘURAREA ANUMITOR TIPURI DE ACTIVITATE.

12.1. Leasing financiar, leasing operațional, împrumuturi acordate persoanelor fizice și juridice.

La adresarea pentru obținerea unui împrumut sau la încheierea unui contract de leasing, clienții (inclusiv garanții) — persoane fizice furnizează Societății, în special: o copie a actului de identitate; informații (adeverințe, extrase sau alte confirmări documentare) privind veniturile; informații privind domiciliul și/sau reședința (înregistrarea); informații privind locul de muncă, funcția și vechimea în muncă; informații privind starea civilă — în volumul necesar evaluării capacității de plată, conform cerințelor de creditare responsabilă; informații privind obiectul leasingului sau o altă garanție a obligației. Clienții — persoane juridice furnizează informații despre reprezentanții, conducătorii și beneficiarii efectivi ai acestora, în

volumul necesar scopurilor încheierii contractului și identificării conform cerințelor Legii nr. 308/2017.

Modul și locul de păstrare a acestor documente: toate documentele enumerate sunt păstrate de Societate pe suport de hârtie — în dulapuri sau seifuri încuiate, amplasate în încăperi de serviciu cu acces limitat — și, concomitent (sau exclusiv), în formă electronică în sistemul informațional securizat, administrat de DSI, cu delimitarea drepturilor de acces ale utilizatorilor și cu jurnalizarea tuturor operațiunilor (vizualizare, modificare, extragere), în conformitate cu art. 32 din Legea nr. 195/2024, care impune Operatorului asigurarea unui nivel de securitate adecvat, ținând cont de risc, inclusiv, după caz, pseudonimizarea și criptarea datelor, asigurarea confidențialității, integrității, disponibilității și rezilienței sistemelor de prelucrare, precum și capacitatea de a restabili în timp util accesul la date în caz de incident.

Termenul de păstrare: minimum 5 (cinci) ani de la încetarea raporturilor contractuale cu clientul, conform legislației privind prevenirea și combaterea spălării banilor și finanțării terorismului (Legea nr. 308/2017), dacă un termen mai îndelungat nu este stabilit de altă legislație aplicabilă (în special, legislația fiscală sau legislația privind prescripția extinctivă) sau nu este necesar pentru apărarea intereselor legitime ale Societății în cadrul unei proceduri judiciare sau administrative.

12.2. Bancassurance (activitate de intermediere în asigurări).

În cadrul prestării serviciilor de bancassurance, datele cu caracter personal ale clientului sunt transmise asigurătorului partener exclusiv în volumul necesar încheierii și executării contractului de asigurare, în baza unui consimțământ separat al clientului sau în cadrul executării contractului de mandat (agenție) încheiat între Societate și asigurător. Societatea încheie cu asigurătorii parteneri acorduri scrise care reglementează condițiile de transmitere, de prelucrare comună și de asigurare a securității datelor cu caracter personal, precum și repartizarea răspunderii pentru respectarea legislației privind protecția datelor cu caracter personal.

12.3. Interacțiunea cu Biroul istoriilor de credit.

Societatea, acționând în calitate de sursă de formare a istoriilor de credit și de utilizator al Biroului istoriilor de credit, transmite date către Birou și obține acces la istoriile de credit ale persoanelor vizate în conformitate cu Legea nr. 122-XVI din 29.05.2008 privind birourile istoriilor de credit, ***exclusiv în baza consimțământului subiectului istoriei de credit*** (sau al unui alt temei legal prevăzut de legea respectivă) și exclusiv în scopurile legate de evaluarea capacității de plată și adoptarea deciziei privind acordarea finanțării.

Accesul la sistemul Biroului istoriilor de credit este acordat unui cerc strict limitat de persoane: doi angajați ai departamentului comercial al Societății și directorul Societății. Fiecare dintre acești angajați acționează sub un login personal (nu comun); istoricul tuturor accesărilor sistemului este jurnalizat automat și face obiectul unei verificări interne periodice (cel puțin o dată pe trimestru) privind justificarea fiecărei accesări și conformitatea acesteia cu scopul declarat al solicitării.

12.4. Interacțiunea cu Cadastrul bunurilor imobile.

Accesul la datele Cadastrului bunurilor imobile (în scopul verificării statutului juridic al obiectului leasingului sau gajului, al existenței unor grevări) se realizează de Societate în conformitate cu Legea nr. 1543-XIII din 25.02.1998 cu privire la cadastrul bunurilor imobile și este acordat aceluiași cerc limitat de persoane ca și accesul la Biroul istoriilor de credit — doi angajați ai departamentului comercial și directorul Societății, cu consemnarea datei, inițiatorului și scopului fiecărei solicitări.

SECȚIUNEA 13. TRANSMITEREA DATELOR CU CARACTER PERSONAL CĂTRE TERȚI ȘI TRANSFERUL TRANSFRONTALIER.

13.1. Datele cu caracter personal pot fi transmise de Societate următoarelor categorii de destinatari și exclusiv în volumul necesar scopului respectiv: Biroul istoriilor de credit; Agenția Servicii Publice (Cadastrul bunurilor imobile); asigurătorii parteneri, în cadrul activității de bancassurance; compania DSI, în calitate de persoană împuternicită care administrează sistemul informațional al Societății; organe de stat — la cerere legală (Centrul Național pentru Protecția Datelor cu Caracter Personal, organele fiscale, organele de urmărire penală și

instanțele de judecată, autoritatea de supraveghere financiară); auditorilor și consultanților profesioniști ai Societății — cu condiția respectării de către aceștia a cerințelor de confidențialitate.

13.2. Transferul transfrontalier de date cu caracter personal (în afara teritoriului Republicii Moldova) este permis doar: către state care asigură un nivel adecvat de protecție a datelor cu caracter personal, recunoscut în modul stabilit; sau în baza unor garanții adecvate, în special clauze contractuale standard, aprobate sau recunoscute de autoritatea competentă; sau în baza unor reguli corporatiste obligatorii (pentru transferul în cadrul unui grup de companii); sau în prezența unui consimțământ explicit și informat al persoanei vizate pentru un asemenea transfer, obținut după explicarea riscurilor posibile. La data aprobării prezentei Politici, Societatea nu efectuează un transfer transfrontalier sistematic al datelor cu caracter personal ale clienților; în cazul apariției unei asemenea necesități (de exemplu, la utilizarea unor servicii informaționale străine), Societatea asigură respectarea cerințelor menționate și documentează temeiul juridic al transferului.

13.3. Cu toate terțele persoane care au calitatea de persoane împuternicite de operator în numele Societății (inclusiv cu DSI) se încheie contracte scrise privind prelucrarea datelor cu caracter personal.

SECȚIUNEA 14. REACȚIA LA ÎNCĂLCĂRILE DE SECURITATE A DATELOR CU CARACTER PERSONAL (INCIDENTE).

14.1. La depistarea de către orice angajat al Societății a unor semne de încălcare a securității datelor cu caracter personal (pierdere, acces neautorizat, divulgare, deteriorare sau distrugere a datelor), angajatul este obligat să informeze de îndată, în cel mult 24 (douăzeci și patru) de ore de la depistare, Responsabilul cu protecția datelor cu caracter personal și administratorul.

14.2. Responsabilul efectuează evaluarea naturii și amplitudinii încălcării, a riscului probabil pentru drepturile și libertățile persoanelor vizate afectate și decide asupra necesității notificării Centrului Național pentru Protecția Datelor cu Caracter Personal și/sau a persoanelor vizate afectate.

14.3. Dacă încălcarea poate genera un risc pentru drepturile și libertățile persoanelor vizate, Societatea notifică Centrul Național în cel mult 72 (șaptezeci și două) de ore de la momentul în care Societatea a luat cunoștință de încălcare, indicând natura încălcării, categoriile și numărul aproximativ al persoanelor vizate și al înregistrărilor afectate, consecințele probabile și măsurile luate sau preconizate pentru remedierea încălcării și diminuarea consecințelor acesteia.

14.4. Dacă încălcarea poate genera un risc ridicat pentru drepturile și libertățile persoanelor vizate, Societatea informează, fără întârzieri nejustificate, persoanele vizate afectate în mod direct, într-un limbaj simplu și clar, cu excepția cazurilor în care se aplică excepțiile prevăzute de legislație (de exemplu, dacă Societatea a luat ulterior măsuri care elimină riscul ridicat).

14.5. Societatea ține Registrul de evidență a incidentelor (încălcărilor de securitate a datelor cu caracter personal), în care se înscriu date despre toate incidentele depistate, indiferent de faptul notificării Centrului Național, inclusiv circumstanțele încălcării, consecințele acesteia și măsurile de remediere luate.

SECȚIUNEA 15. DATELE CU CARACTER PERSONAL PE SITE-UL OFICIAL AL SOCIETĂȚII.

15.1. Site-ul oficial al Societății trebuie să conțină:

- toate datele de identificare ale Operatorului: denumirea, IDNO, sediul, datele de contact, inclusiv contactul Responsabilului cu protecția datelor cu caracter personal (e-mail/telefon direct al Responsabilului cu protecția datelor);
- Politica de confidențialitate accesibilă clienților (poate fi un extras sau o versiune adaptată a prezentei Politici), care descrie scopurile și temeiurile juridice ale prelucrării datelor vizitatorilor site-ului, categoriile de date prelucrate, termenele de păstrare, categoriile de destinatari, drepturile persoanelor vizate și modul de exercitare a acestora, precum și faptul și condițiile transferului transfrontalier de date (dacă este cazul);
- o descriere onestă, completă și care nu induce în eroare a condițiilor de prestare a serviciilor financiare (leasing, împrumuturi) — rata dobânzii, dobânda anuală efectivă, costul total al creditului, alte condiții esențiale — în

conformitate cu legislația privind protecția consumatorilor și creditarea responsabilă.

15.2. Site-ul oficial al Societății nu trebuie să conțină (și nu admite):

- formulare de colectare a datelor cu caracter personal care solicită un volum de informații excesiv în raport cu scopul declarat al adresării (de exemplu, solicitarea de date privind starea de sănătate sau naționalitatea la depunerea unei simple cereri de consultanță);
- căsuțe bifate în prealabil privind consimțământul pentru prelucrarea datelor în scopuri de marketing sau pentru transmiterea datelor către terți — consimțământul trebuie să fie rezultatul unei acțiuni active a utilizatorului;
- date cu caracter personal ale clienților (fotografii, nume și prenume, recenzii, descrieri ale unor tranzacții concrete, sume de finanțare) fără un consimțământ scris separat, confirmat documentar, al clientului respectiv pentru o astfel de publicare, cu păstrarea dreptului clientului de a revoca în orice moment un asemenea consimțământ și de a solicita eliminarea materialului;
- conectarea unor instrumente de urmărire terțe, pixeli ai rețelelor sociale și servicii analitice înainte de obținerea consimțământului utilizatorului pentru categoria respectivă de fișiere cookie;
- informații care induc în eroare privind condițiile de prelucrare a datelor cu caracter personal, precum și afirmații false privind „anonimitatea completă” a vizitării site-ului sau „lipsa colectării de date”, dacă în realitate o asemenea colectare are loc (de exemplu, prin fișiere cookie tehnice sau înregistrarea adresei IP);
- funcționalități de adoptare a unor decizii complet automatizate (de exemplu, aprobarea sau respingerea automată a unei cereri de împrumut fără intervenție umană), care afectează drepturile și interesele legitime ale persoanei vizate, fără informarea prealabilă a acesteia și fără asigurarea dreptului acesteia la reexaminarea deciziei de către o persoană.

SECȚIUNEA 16. EXAMINAREA SESIZĂRILOR ȘI RECLAMAȚIILOR PERSOANELOR VIZATE.

16.1. Societatea asigură recepționarea, înregistrarea și examinarea în timp util a sesizărilor (cererilor, reclamațiilor, plângerilor) persoanelor vizate legate de prelucrarea datelor acestora, primite în formă scrisă — prin e-mail, prin formularul de pe site-ul oficial, prin poștă sau personal, la sediul Societății.

16.2. Fiecare sesizare primită se înregistrează obligatoriu în Registrul de evidență a sesizărilor persoanelor vizate în ziua primirii, cu atribuirea unui număr de înregistrare și indicarea datei primirii.

16.3. Răspunsul Societății la sesizare (corespondența cu persoana vizată) trebuie să conțină:

- numărul și data înregistrării sesizării, precum și data întocmirii răspunsului;
- expunerea esenței cererii formulate, așa cum a fost înțeleasă de Societate, pentru a evita interpretările divergente privind obiectul sesizării;
- o indicație clară privind satisfacerea (integrală sau parțială) sau refuzul motivat de a satisface cererea formulată, cu descrierea acțiunilor concrete întreprinse (de exemplu, rectificarea sau ștergerea datelor, copia datelor transmisă) sau a temeiului juridic și factologic al refuzului;
- în caz de refuz — trimiterea exactă la temeiul juridic al refuzului (de exemplu, necesitatea păstrării datelor pentru îndeplinirea unei obligații legale conform Legii nr. 308/2017 privind PSB/FT, pentru constatarea, exercitarea sau apărarea unor pretenții legale ale Societății, sau pentru respectarea legislației arhivistice), cu trimitere la articolul concret al legii respective;
- explicarea dreptului persoanei vizate de a depune o plângere la Centrul Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova și/sau de a se adresa instanței de judecată, cu indicarea datelor de contact ale Centrului;
- datele de contact ale Responsabilului cu protecția datelor cu caracter personal al Societății pentru o eventuală comunicare ulterioară privind esența sesizării;
- semnătura reprezentantului împuternicit al Societății și data semnării răspunsului.

16.4. Răspunsul la sesizare se transmite persoanei vizate în cel mult o lună de la data primirii acesteia de către Societate. Acest termen poate fi prelungit cu încă două luni, ținând cont de complexitatea și numărul sesizărilor primite, persoana vizată fiind informată despre prelungirea termenului și despre motivele acesteia în cursul primei luni de la primirea sesizării.

16.5. Corespondența privind sesizarea nu trebuie să conțină:

- date cu caracter personal ale altor persoane (terți) care nu au legătură directă cu esența sesizării solicitantului (de exemplu, la examinarea unei sesizări privind un contract cu un cobeneficiar de împrumut — date ale cobeneficiarului în afara volumului necesar răspunsului către solicitant);
- un volum de informații excesiv pentru scopurile verificării identității solicitantului — Societatea nu este în drept să solicite copii ale actelor de identitate peste ceea ce este necesar pentru identificarea univocă, cu excepția cazurilor unor îndoieli întemeiate privind identitatea solicitantului;
- formulări de refuz neargumentate, standard, fără indicarea motivelor concrete și a temeiului juridic exact.

16.6. Toate sesizările și răspunsurile la acestea, precum și informațiile privind măsurile luate, se păstrează de Societate minimum 5 (cinci) ani de la data înregistrării sesizării — în scopul confirmării respectării principiului responsabilității (art. 5 din Legea nr. 195/2024), precum și în scopul monitorizării și identificării problemelor sistemice în procesele de prelucrare a datelor cu caracter personal ale Societății.

SECȚIUNEA 17. RĂSPUNDEREA PENTRU ÎNCĂLCAREA CERINȚELOR LEGISLAȚIEI PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL ȘI A PREZENTEI POLITICI.

17.1. Angajații Societății vinovați de încălcarea cerințelor legislației privind protecția datelor cu caracter personal și/sau ale prezentei Politici poartă răspundere disciplinară, care poate merge până la concediere în temeiurile corespunzătoare prevăzute de Codul muncii al RM, răspundere materială pentru prejudiciul cauzat Societății, precum și, în funcție de natura încălcării, răspundere contravențională în

conformitate cu Codul contravențional al RM și răspundere penală în conformitate cu Codul penal al RM (în special, pentru colectarea ilegală sau răspândirea intenționată a unor informații ce constituie taină personală sau de familie a unei persoane, fără consimțământul acesteia).

17.2. Societatea, în calitate de Operator de date cu caracter personal, poartă răspundere pentru încălcarea cerințelor Legii nr. 195/2024 sub formă de avertisment, sau după caz amenzi bănești, aplicate de Centrul Național pentru Protecția Datelor cu Caracter Personal în conformitate cu art. 88 din Legea nr. 195/2024.

SECȚIUNEA 18. DISPOZIȚII FINALE.

18.1. Prezenta Politică intră în vigoare la data aprobării ei prin ordinul directorului Societății.

18.2. Revizuirea și actualizarea prezentei Politici se efectuează cel puțin o dată pe an, precum și în cazul modificării legislației Republicii Moldova privind protecția datelor cu caracter personal, al modificării tipurilor de activitate ale Societății, al implementării unor noi sisteme informaționale sau în urma unui audit efectuat ori a unui incident depistat. Răspunderea pentru inițierea revizuirii și pregătirea modificărilor revine Responsabilului cu protecția datelor cu caracter personal.

18.3. În cazul unei contradicții între prevederile prezentei Politici și legislația în vigoare a Republicii Moldova, se aplică normele legale.

18.4. Angajații Societății poartă răspundere pentru încălcarea prevederilor prezentei Politici în conformitate cu legislația muncii a Republicii Moldova și cu actele normative interne ale Societății.

18.5. Prezenta Politică este accesibilă pentru consultare tuturor angajaților Societății, iar versiunea actualizată a acesteia este plasată pe site-ul oficial al Societății și în locuri accesibile pentru consultare de către angajați (portal intern/panou informativ).