

PRIVACY NOTICE

I. PURPOSE

- 1.1 This Privacy Notice explains how **O.C.N. “IUTE CREDIT” S.R.L.** (“**Iute**”, “**we**”, “**us**”) Processes Personal Data about individuals (“**you**”) when you use our services or interact with us, including through our website, MyIute app, customer support channels (including customer service phone, chatbots), branches, loan intermediaries, and other channels we make available (together, the “**Available Channels**”).
- 1.2 Please read this Notice carefully before submitting your Personal Data to us. By providing your Personal Data, you acknowledge that you have read and understood this Notice.
- 1.3 Our use of cookies and similar technologies is described in a separate Cookie Notice.
- 1.4 Our services are not available to persons under the age of 18. We do not offer, provide or enter into agreements for our services with persons under the age of 18.

II. WHO WE ARE

- 2.1. For the purposes of the GDPR, the data Controller is **O.C.N. “IUTE CREDIT” S.R.L.** , 1008600026223, Bd.Ștefan ce Mare și Sfânt 182, floor 5., 2004 Chisinau, Republica Moldova.
- 2.2. We also act as a joint controller together with **Iute Group AS** (Estonia). We manage customer contact and our service delivery, while Iute Group AS provides IT systems, infrastructure, backups, security, analytics, and strategic oversight. Where needed, Iute Group AS may Process your Personal Data for platform management, service improvement, analytics, compliance, and security.
- 2.3. A summary of the relevant joint controllership arrangements is available upon request by contacting the details below.

O.C.N. “IUTE CREDIT” S.R.L. (1008600026223)	
Bd.Ștefan ce Mare și Sfânt 182, floor 5., 2004 Chisinau, Republica Moldova	E-mail: dpo@iute.md
Iute Group AS (11551447)	
Maakri 19/1, Tallinn, 10145 Estonia	E-mail: dpo@iute.com

III. DEFINITIONS

- 3.1. **Customer** (or **you**) means any natural person who uses, has used, or has expressed an interest in using Iute’s services or products, or who is otherwise connected to Iute, its services, or its Customers, including as a legal or authorized representative, heir, guarantor, or user or visitor of Iute’s Available Channels. This Notice also applies to Customer relationships established before the Notice entered

into force. Customers have all rights granted to data subjects under the General Data Protection Regulation (EU) 2016/679 (“**GDPR**”).

- 3.2. **Iute Group** means Iute Group AS, a public limited company incorporated in Estonia, and all legal entities in which Iute Group AS has direct or indirect controlling influence (subsidiaries).
- 3.3. **Customer Data** is any Personal Data known to Iute about a Customer.
- 3.4. **Personal Data** means means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
- 3.5. **Processing** means any operation or set of operations that is performed with Customer Data, either by automated or non-automated means, such as collection, storage, organization, retention, adaptation, modification, consultation, use, combination, deletion, or destruction.
- 3.6. **Controller** is someone who, alone or jointly with others, determines the purposes and means of Processing Customer Data. For more information, see Section II of this Notice.
- 3.7. **Recipient** is a natural or legal person, a public sector institution, or another body to whom Iute has the right to disclose Customer Data. Recipient categories are described in more detail in Section IX of this Notice.
- 3.8. **Processor** is a natural or legal person who Processes Customer Data on behalf of Iute. Iute engages Processors for the Processing of Customer Data and takes the necessary steps to ensure that the authorized Processors Process Customer Data based on an agreement or Applicable Laws and in accordance with Iute’s documented instructions.
- 3.9. **Applicable Laws** means all legal acts, rules, and guidelines applicable to Iute, including legislation on the data protection, prevention of money laundering and terrorist financing, business activities, taxes, accounting, and other activities.

IV. DATA WE COLLECT

- 4.1. Iute collects following Customer Data:

Category	Examples of Customer Data we may Process
Identification and verification details	Name, gender, personal identification code, date of birth, legal capacity information where required, and identity document data, including checks of identity document validity. Where identity verification is completed remotely, we may process images or video recordings of you and your identity document, as well as liveness-check results. Where facial images are processed for the purpose of

Category	Examples of Customer Data we may Process
	uniquely identifying you, we may also process biometric data derived from those images.
Contact details	Address, email address, telephone number(s), and preferred language of communication.
Representation and related-party details	Information about representatives, authorized persons, contact persons, guarantors, collateral providers, including name, contact details, ID data, authority and relationship to the Customer.
Family, household, and demographic data	Citizenship, nationality, and similar information where permitted and necessary for the relevant service or product.
Professional and employment data	Education, professional career, employer, position, length of service, employment status, remuneration, other income, and related employment information where permitted and necessary.
Financial, account, and loan data	Income, expenses, liabilities, assets, property status, bank account number, card or direct debit details where you choose such repayment method, selected loan disbursement method, loan agreement number, loan amount, repayment schedule, repayments, overdue amounts, fees, arrears, restructuring data and other loan servicing information.
Creditworthiness, affordability, and loan servicing data	Credit history, repayment behavior, arrears, information about existing or previous loans, health-insurance information, information obtained from credit registers, social security or employment registers, civil or population registers, identity document registers, property registers, and similar sources where applicable in the relevant country and permitted by law.
KYC, AML, sanctions, and due diligence data	Identity-verification, customer due-diligence and risk-assessment data; information on the purpose and nature of the customer relationship, politically exposed persons, sanctions, suspicious activity, and, where required, the origin of funds or assets.
Communication, support, and recording data	Phone calls, emails, chats, chatbots, messages, social media interactions, complaints, service requests, visit records, branch CCTV or visual recordings where permitted, call recordings and related metadata such as time, channel, delivery status and support case details.
Technical and usage data	Device identifiers and signature data, IP address, date and time of access, activity in Available Channels, cookie preferences, domain name, software and hardware attributes, approximate location such as city and country, operating system, language settings, network type, app usage patterns, engagement metrics and similar technical metadata.
Marketing, preferences and satisfaction data	Marketing consents and opt-outs, product interests, preferences, survey responses, campaign participation, customer satisfaction results and interaction history with offers.
Legal, regulatory and claims data	Data required to comply with legal obligations, respond to authorities, maintain records, report to regulators, conduct audits, manage

Category	Examples of Customer Data we may Process
	disputes, establish, exercise or defend legal claims, and protect the rights and property of Iute, customers or third parties.

V. WHY WE PROCESS PERSONAL DATA

5.1. Below we explain the main purposes for which we Process Personal Data, the types of data used for each purpose, and the legal basis for Processing.

Purpose	Examples of Processing	Legal basis
Identification and authentication	Identifying you, verifying your identity document, verifying a representative or authorized person, authenticating access to MyIute and other Available Channels.	Legal obligation; contract; legitimate interest; Consent where required.
KYC, AML, counter-terrorist financing and sanctions compliance	Customer due diligence, ongoing monitoring, identifying politically exposed persons or sanctioned persons, monitoring suspicious behaviour and meeting reporting obligations.	Legal obligation; legitimate interest where permitted.
Loan application assessment	Receiving and processing loan applications, checking eligibility, assessing whether to enter into a loan agreement and on what terms.	Contract; legal obligation; legitimate interest.
Creditworthiness, affordability and responsible lending	Assessing income, expenses, existing obligations, credit history, repayment ability, risk level and responsible lending requirements.	Legal obligation; legitimate interest; Consent where register access requires it.
Loan agreement performance and servicing	Concluding, amending, performing and terminating loan agreements, disbursing loan funds, receiving repayments, managing repayment schedules, fees, arrears, restructuring and customer relationship records	Contract; legal obligation; legitimate interest.
Credit-register and payment-default reporting	Information obtained from credit or payment-default registers and, where permitted or required by Applicable Law, information reported to such registers about your customer relationship, payment performance, overdue amounts, arrears and payment defaults, including updates or corrections to previously reported information.	Legal obligation; legitimate interest where permitted; Consent where required by Applicable Law for access to a specific register.

Purpose	Examples of Processing	Legal basis
Fraud prevention, security and misuse prevention	Detecting and preventing identity fraud, account misuse, cyber threats, unauthorized access, service disruption, unlawful activity and damage to Iute, customers or third parties.	Legal obligation; legitimate interest; Consent where required.
Customer support and communications	Responding to requests, complaints and questions, providing service information, maintaining communication records, call recordings and chat histories.	Contract; legal obligation; legitimate interest; Consent where required.
Website, app and digital channel operation	Providing website and app functionality, secure login, service availability, system logs, troubleshooting, cookie preferences and essential technical processing.	Contract; legitimate interest; legal obligation; consent for non-essential cookies.
Pre-filling application and service fields	Automatically populating certain fields, such as contact details, with information previously provided by the customer, to reduce repeated data entry and improve the customer experience. Customers can review and correct the information before submission.	Legitimate interest.
Service improvement, analytics and business reporting	Developing and improving services, systems, risk models and customer experience, measuring performance and preparing statistical reports, using aggregated or pseudonymous data where possible.	Legitimate interest; consent where required.
Marketing and customer engagement	Sending offers, campaigns, surveys and information about Iute and its partners' products and services, and measuring campaign effectiveness.	Consent where required; legitimate interest for permitted direct marketing to existing customers; right to object or opt out.
Legal claims, audits and regulatory reporting	Maintaining evidence, conducting internal controls and audits, responding to courts, authorities and regulators, and establishing, exercising or defending legal claims.	Legal obligation; legitimate interest; legal claims; public interest where applicable.

VI. DO I HAVE TO PROVIDE MY PERSONAL DATA?

- 6.1. In some cases, you must provide Personal Data because it is required by law or necessary for us to assess your application, enter into or perform an agreement with you, verify your identity, prevent fraud, or comply with our legal obligations.

- 6.2. If you do not provide the required data, we may be unable to process your application, provide the requested service, enter into or continue the customer relationship, or comply with our legal obligations. Providing data for marketing and other optional purposes is voluntary.

VII. USE OF ARTIFICIAL INTELLIGENCE

- 7.1. We use Artificial Intelligence (AI) responsibly and ethically, always respecting your privacy and ensuring compliance with the Applicable Laws. Our AI systems are used for clearly defined purposes for example such as enhancing customer support through automated assistance, improving the accuracy of data analysis, risk and business management purposes, and detecting security risks. We do not use AI to make decisions that produce legal or similarly significant effects on you without providing meaningful human involvement, a lawful basis, and all rights afforded to you under the Applicable Law. All AI driven activities are subject to appropriate technical and organizational safeguards, human oversight, and strict compliance with Applicable Laws.

VIII. PROFILING AND AUTOMATED DECISION-MAKING

- 8.1. We may use profiling and, where permitted by law, automated decision-making to assess applications, manage credit risk, prevent fraud, and meet anti-money laundering obligations. This may involve evaluating information such as identification details, creditworthiness data, repayment history, device and usage information, and interactions across our Available Channels.
- 8.2. Profiling or automated tools may influence the checks we perform, the information we request, the level of verification required, the proposed terms of a service or agreement, or the risk controls applied. No decision that produces legal effects concerning you, or similarly significantly affects you, is made solely by automated means. A trained employee reviews the relevant information and is able to reassess the outcome.

IX. COLLECTING AND SHARING PERSONAL DATA

9.1. Sources Of Customer Data

- 9.1.1. Iute collects Customer Data directly from the Customer, Iute Group companies and Available Channels, and from external sources where this is necessary for the preparation, conclusion, performance, or administration of an agreement, or for the provision and use of Iute's services.
- 9.1.2. External sources may include public registers, such as Credit Bureaus, the Public Services Agency, the National Health Insurance Company, etc.
- 9.1.3. Iute may also collect and Process Customer Data by recording or documenting communications between the Customer and Iute. This may include phone calls, emails, visual images, video and/or audio recordings, online or in-person communications, and other forms of interaction with Iute.

9.1.4. Where Personal Data collected through such sources or communications is not necessary, relevant, or suitable for the purpose for which it was collected, Iute will not Process it further and will delete or anonymize it where possible, unless retention is required by Applicable Law.

9.2. Recipients of Customer Data

9.2.1. Iute may disclose Customer Data to Recipients where this is necessary to provide services, support business operations, prepare, conclude, perform, or administer agreements, assess creditworthiness, comply with legal or regulatory obligations, prevent fraud, ensure security, manage arrears, or establish, exercise, or defend legal claims.

9.2.2. Recipients to whom Iute may disclose Customer Data include:

- Iute Group companies, where they process Personal Data for group-level governance, compliance, audit, risk management, reporting, security, legal, finance, analytics, or other legitimate group purposes;
- banks, credit and payment institutions, payment intermediaries, repayment-processing partners and international card organizations, for loan disbursement, payment processing and repayment administration;
- credit bureaus, credit-history and other relevant public or private registers, where data is obtained or reported for creditworthiness assessment, responsible lending, identity or data verification and compliance with legal obligations;
- loan intermediaries, partners, merchants, guarantors, collateral providers, authorized representatives and other persons involved in the Customer relationship or performance of the Customer's obligations;
- service providers, including providers of IT, communications, hosting, cloud, postal, call-centre, customer-support, video-surveillance, archiving, printing and other technical or operational services;
- marketing partners and insurance companies or brokers, where disclosure is necessary for marketing based on an appropriate legal basis or for arranging, administering or providing insurance-related services;
- debt collection providers, creditors, prospective purchasers or assignees, new creditors, insolvency administrators, bailiffs, legal advisers, auditors and other professional advisers, where necessary for debt recovery, transfer of agreements or claims, audits or legal proceedings; and
- courts, notaries, law-enforcement, tax, supervisory, regulatory, data-protection and other competent public authorities, where disclosure is required or permitted by Applicable Laws.

9.2.3. Iute's Processors include:

- legal persons belonging to the Iute Group and their branches if they Process Customer Data on behalf of Iute.
- other persons involved in the provision of services to Iute, such as providers of video surveillance, information technology, web hosting, cloud computing, archiving and printing services, technical experts and assessors.

X. GEOGRAPHICAL AREA OF PROCESSING

10.1. As a general rule, Customer Data is processed in Republic of Moldova and in the EU/EEA. Iute shall only transfer Customer Data outside EU/EEA if there is a legal basis for this and a lawful transfer mechanism is in place, in accordance with Applicable Laws. Such mechanisms may include where appropriate:

- [An adequacy decision from the European Commission](#), confirming that the third country ensures an adequate level of data protection; or
- in the absence of an adequacy decision, appropriate safeguards, such as [the Standard Contractual Clauses \(SCCs\) adopted by the European Commission](#), implemented between the Iute entity and a recipient.
- There are derogations for specific situations, such as the Customer's explicit Consent; the performance of an agreement with the Customer; the conclusion or performance of an agreement with a third party in the interest of the Customer; the establishment or defense of legal claims; or important grounds of public interest.

10.2. We may also implement additional technical and organizational measures to protect data during and after transfer, based on what is effective and technically feasible.

10.3. You may request further information about international transfers and the safeguards used to protect your Personal Data by contacting us using the details in Section II.

XI. HOW WE PROTECT YOUR PERSONAL DATA

11.1. We apply appropriate technical, organisational and physical measures to protect Personal Data against unauthorized or unlawful access, use, disclosure, alteration, loss or destruction. These measures are determined taking into account the nature of the Personal Data, the Processing involved and the relevant security risks.

11.2. Depending on the nature of the Processing and the relevant risks, our security measures may include access controls and authentication, technical protection and monitoring, system maintenance and security testing, backup and recovery arrangements, physical safeguards, confidentiality and security requirements for personnel, and internal security policies and procedures.

- 11.3. We also take measures designed to protect the confidentiality, integrity and availability of our website, MyIute and other digital Available Channels. Where appropriate, we may use authentication controls, verification mechanisms, device-related information, monitoring and other security measures to protect accounts and services and to detect or prevent unauthorized access, fraud, misuse or other security threats.
- 11.4. Personal Data may be stored or Processed in systems operated by Iute, other Iute Group companies or service providers acting on our behalf. Where third parties have access to Personal Data or systems used to Process Personal Data, we apply appropriate contractual, organisational and other safeguards according to the nature of the Processing and relevant risks.
- 11.5. If a security incident involves Personal Data, we assess and respond to the incident according to its nature, scope and potential impact. Measures may include containment, investigation, remediation, restoration of affected services and implementation of additional safeguards. Where required by Applicable Laws, we will also notify competent authorities and/or affected individuals.
- 11.6. Security risks, technologies and threats develop over time. We therefore review and, where appropriate, update our security measures, policies and procedures to reflect changes in our systems, operations, risks and Applicable Laws.
- 11.7. You can also help protect your Personal Data by keeping your passwords, PINs and verification codes confidential, keeping your devices and applications reasonably up to date, being alert to phishing or fraudulent communications, and using official Iute channels when accessing our services or sharing sensitive information. Please inform us promptly if you believe that your account, credentials or communications with Iute have been compromised or used without your authorization.

XII. DATA RETENTION

- 12.1. Iute stores Customer Data collected during the business relationship after the end of the business relationship. Iute stores Customer Data based on the retention periods provided by legislation for the preparation and submission of claims or a legitimate interest in order to protect the interests of Iute.
- 12.2. At the end of the applicable retention period, we will securely delete, anonymise or otherwise irreversibly destroy Personal Data, unless continued retention is required by Applicable Law or is necessary to establish, exercise or defend legal claims.

XIII. YOUR RIGHTS

- 13.1. To the extent required by applicable data protection regulations, you have all the rights of a data subject as regards your Customer Data. Such rights include the following:
- Right to access - know what Customer Data we hold and obtain a copy.
 - Right to rectification - correct inaccurate or incomplete data.
 - Right to erasure ("right to be forgotten") - request deletion under certain conditions.
 - Right to restrict processing - suspend processing under specific circumstances.

- Right to data portability - receive your data in a structured, commonly used format.
- Right to object - to processing based on legitimate interest.
- Right to withdraw consent - at any time without affecting past lawful processing.
- Right to lodge a complaint - with us or a supervisory authority (see below).

13.2. We will respond to your request without undue delay and, in any event, within one month of receiving it. Where permitted by Applicable Law, we may extend this period by up to two further months, and will notify you of the extension and the reasons for it within the initial one-month period. No fee is required unless requests are unfounded or excessive.

13.3. To exercise your rights, contact us at dpo@iute.md. You will not be discriminated against for exercising any of your rights.

XIV. COMPLAINTS

14.1. If you believe your rights have been violated, you can contact us at dpo@iute.md or lodge a complaint with the National Center for Personal Data Protection of the Republic of Moldova.

- Email: centru@datepersonale.md
- Website: <https://datepersonale.md/en/>

XV. CHANGES TO THIS NOTICE

15.1. We reserve the right to update this Notice. All changes will be posted on this page, and significant changes will be communicated via our website and/or app.

Last updated: 25.08.2026