Privacy Policy

Effective Date: 29 May 2026

1. Introduction

LOANCH is a platform where investors can acquire credit claims originated by our lending partners. When you use the platform (browsing, registering, investing) we collect and use information about you. This Policy tells you what we collect, why we collect it, and what you can do about it.

EU data protection law requires us to give you this information in writing. We've tried to write it so it's actually useful, not just complete. The sections most likely to matter to you day-to-day: Section 8 (why we use your data), Section 10 (how Auto Invest handles your account automatically), Section 11 (how long we keep things), and Section 17 (your rights).

If something isn't clear, email dpo@loanch.com.

2. Who We Are

LOANCH is operated by PRZEMEK SAVJETOVANJE d.o.o., registered in Croatia (company number 49535909257), with its registered office at Kačićeva ulica 2, 10000 Zagreb. We're the data controller: we decide how and why your personal data is processed in connection with the platform and its services.

Where third parties are involved in delivering our services (identity verification providers, payment processors, loan originators) they may handle your data either on our behalf or as independent controllers in their own right. Where that distinction matters, we flag it in the relevant section of this Policy.

3. How to Contact Us

For questions about this Policy, or how we handle your data, contact us at:

Email: dpo@loanch.com

Post: PRZEMEK SAVJETOVANJE d.o.o., Kačićeva ulica 2, 10000 Zagreb, Croatia

This is also where to send requests to exercise your rights under Section 17.

4. Who This Privacy Policy Applies To

This Policy applies to anyone who interacts with LOANCH: website visitors, people going through registration or account opening (whether or not they complete it), active investors, and corporate clients including their directors, beneficial owners, and authorised representatives.

It also covers individuals whose data we receive through compliance processes such as KYC checks, AML screening, and sanctions reviews, even if those people haven't directly signed up with us.

If you contact us by email, support form, or any other channel, this Policy applies to the data you share in those communications.

Third parties involved in delivering our services (banks, verification providers, loan originators) operate under their own privacy policies when they act as independent controllers. This Policy doesn't govern what they do with your data.

5. Categories of Personal Data We Collect

What we collect depends on how you use LOANCH: a website visitor shares less than a registered investor, and a corporate client more than an individual.

5.1 Website visitors

When you browse loanch.com without an account, we collect basic technical data: your IP address, browser type, device, and how you navigate the site. We also use cookies. See our Cookie Policy for details on what those track and how to manage them.

5.2 Account registration and onboarding

Opening an account means sharing quite a bit. We collect:

- identity data: name, date of birth, nationality, and ID document details and copies;
- contact data: email address, phone number, and residential address;
- login credentials and account preferences;
- tax residency information and any relevant tax certificates;
- documents and declarations you submit during onboarding; and
- KYC and AML compliance data required by law.

5.3 Investment activity

For active investors, we additionally collect:

- financial profile: source of funds, financial situation, and capacity to bear losses;
- investment preferences and appropriateness assessment responses;
- transaction records: amounts, dates, account balances, payment details, and returns;
- contractual records: assignment agreements, confirmations, and acceptance logs; and
- support history: messages, complaints, and account correspondence.

5.4 Compliance and risk

Some data we hold primarily for regulatory reasons:

- AML screening results, PEP status, sanctions checks, and due diligence findings;
- fraud and security signals: login history, device data, and suspicious activity flags;
- beneficial ownership information for corporate accounts; and
- records needed for tax, accounting, and regulatory reporting.

5.5 Marketing and communications

If you receive communications from us, we hold your email address, your preferences (subscribed or unsubscribed), and basic engagement data such as whether emails were delivered and opened.

5.6 Corporate clients

If you act on behalf of a company, we collect information about you personally (identity, role, and authority) and about the organisation: its ownership structure, directors, beneficial owners, and compliance-related information.

5.7 Data you send us

Anything you include in a message, support ticket, or uploaded file — we hold that too. Keep it relevant to whatever you're asking us about.

6. How We Collect Personal Data

Most comes directly from you. Some we collect automatically. Some we receive from third parties. Here's how each works.

6.1 Directly from you

Most of the data we hold comes from you: when you register, complete onboarding, invest, contact support, or just send us a message. That includes everything you type into forms, documents you upload, and anything you communicate through any channel.

6.2 Automatically

When you use our website or platform, we collect technical data automatically through cookies, server logs, and similar tools. This covers things like your IP address, which pages you visit, and how long you spend on them. We use it to keep the platform running, detect problems, and understand how it's being used. See our Cookie Policy for the full picture.

6.3 During compliance checks

As part of onboarding and ongoing account monitoring, we may verify the information you provide against third-party sources such as identity databases, sanctions lists, and PEP registries. This is required by anti-money laundering law and our own compliance procedures.

6.4 From third parties

We also receive data from identity verification providers, payment processors, corporate registries, and similar sources. Section 7 explains this in more detail.

6.5 Data we generate

Some records we generate ourselves: audit trails, compliance notes, risk assessments, and account status logs. These reflect your activity on the platform and our regulatory obligations.

7. Personal Data Obtained from Third Parties

We don't rely only on what you tell us directly. For compliance, account administration, and transaction processing, we also receive data from external sources.

7.1 Identity verification and compliance providers

We use third-party KYC, AML, and sanctions screening services to verify identities and check for risk. These providers return verification results, document validation outputs, and screening flags that feed into our onboarding and ongoing compliance processes.

7.2 Public registers and official sources

We check publicly available sources including corporate registers, sanctions lists, PEP databases, insolvency registers, and beneficial ownership registers to verify information and meet our due diligence obligations.

7.3 Banks and payment providers

Account funding, withdrawals, and payment verification involve banks and payment processors, who share transaction-related data with us as part of those processes.

7.4 Business partners and counterparties

If a specific deal or service involves a counterparty or business partner, they may share information about you with us as part of that arrangement.

7.5 Your organisation

If you're acting on behalf of a company, we may receive information about you from that company or from others involved in the same transaction, such as signatories, beneficial owners, or advisers.

7.6 Other lawful sources

We may also receive data from other sources where the law permits, for example to investigate suspected fraud or respond to requests from competent authorities.

If we receive your personal data from a third party rather than directly from you, we'll tell you what we received, where it came from, and why we're using it, as required under Article 14 GDPR.

8. Purposes of Processing and Legal Bases

EU law requires us to have a specific legal basis for each use of your data. The table below sets out what we use your data for and which basis applies. In practice, more than one basis can cover the same activity. KYC checks, for example, are both a legal obligation and a legitimate interest.

Purpose of processing	**Categories of personal data typically involved**	**Legal basis**
Website operation	Technical, device, and usage data; cookie data	Art. 6(1)(f) – legitimate interest in operating and securing our website
Account creation and management	Identity, contact, and account data	Art. 6(1)(b) – contract performance

Onboarding and application assessment	Identity, contact, document, tax, financial profile, and compliance data	Art. 6(1)(b) – pre-contractual steps; Art. 6(1)(c) – legal obligation; Art. 6(1)(f) – legitimate interest
KYC, AML, sanctions, and fraud checks	Identity and document data, source of funds, PEP status, sanctions results, risk indicators	Art. 6(1)(c) – legal obligation; Art. 6(1)(f) – legitimate interest in preventing fraud
Investor assessment and appropriateness testing	Financial profile, investment data, questionnaire responses	Art. 6(1)(b) – contract; Art. 6(1)(c) – legal obligation; Art. 6(1)(f) – legitimate interest
Investment services and contract administration	Identity, contact, transaction, contractual, and account data; support records	Art. 6(1)(b) – contract; Art. 6(1)(c) – legal obligation
Payments, withdrawals, and transaction records	Identity, transaction, and payment data; bank account details	Art. 6(1)(b) – contract; Art. 6(1)(c) – legal obligation
Account and service communications	Contact, account, transaction, and support data	Art. 6(1)(b) – contract; Art. 6(1)(c) – legal obligation; Art. 6(1)(f) – legitimate interest
Enquiries, complaints, and feedback	Identity, contact, communications, and case records	Art. 6(1)(b) – contract; Art. 6(1)(f) – legitimate interest; Art. 6(1)(c) – where required
Record-keeping, accounting, and regulatory reporting	Identity, transaction, contractual, tax, and compliance records	Art. 6(1)(c) – legal obligation; Art. 6(1)(f) – legitimate interest
Platform security, maintenance, and improvement	Technical, usage, and log data; error reports; internal analytics	Art. 6(1)(f) – legitimate interest in operating and improving our services
Fraud prevention and security	Identity, technical, and device data; login history; risk signals	Art. 6(1)(c) – legal obligation; Art. 6(1)(f) – legitimate interest
Legal claims and enforcement	Identity, transaction, contractual, and communications data; relevant evidence	Art. 6(1)(f) – legitimate interest; Art. 6(1)(c) – where required
Authority requests and legal obligations	Any data relevant to the request	Art. 6(1)(c) – legal obligation
Marketing communications	Contact data, marketing preferences, engagement data	Art. 6(1)(a) – consent; Art. 6(1)(f) – legitimate interest
Consent and suppression management	Contact data, consent records, opt-in/opt-out data	Art. 6(1)(c) – legal obligation; Art. 6(1)(f) – legitimate interest
Surveys, events, and campaigns	Identity, contact data, participation records	Art. 6(1)(a) – consent; Art. 6(1)(f) – legitimate interest

Legitimate interests: when we rely on this basis, the interests at stake are running and improving the platform, preventing fraud, managing our relationship with you, keeping records, and protecting our legal rights.

Consent: you can withdraw it at any time. This won't affect anything we did before you withdrew. If you don't provide data we need to perform a contract or meet a legal obligation, we may not be able to offer you the relevant service.

9. Special Categories of Personal Data and Criminal-Offence Related Data

LOANCH doesn't collect sensitive personal data (health information, biometric data, religious beliefs, and similar categories covered by Article 9 GDPR) as part of its standard services.

That said, it can happen. If you volunteer information that falls into a sensitive category, or if such data surfaces during KYC, AML screening, or sanctions checks, we'll process it only to the extent required by the relevant compliance obligation, with an appropriate legal basis in place, and never for marketing purposes.

We also process data relating to criminal records and sanctions exposure for AML and counter-terrorist financing purposes. This is a legal requirement. The same restrictions apply: appropriate legal basis, access controls, data minimisation, no use for marketing.

10. Automated Decision-Making and Profiling

10.1 Auto Invest

Auto Invest is an optional feature that automatically allocates funds from your LOANCH account into available credit claims, without requiring you to review and approve each transaction individually.

When you activate Auto Invest, you configure your investment parameters: for example, the interest rate range, maximum exposure per claim, originator preferences, and loan term. Once activated, our systems scan the marketplace for claims that match those parameters and execute Assignment Agreements on your behalf when a match is found. Each execution has real legal consequences: funds are debited from your account and you become the assignee of the relevant claim.

This is automated decision-making that produces legal effects within the meaning of Article 22 GDPR. We carry it out on the basis of your explicit prior instruction: by activating Auto Invest and confirming your parameters, you're directing us to act automatically within the boundaries you've set.

You can pause or deactivate Auto Invest at any time through your account settings. Deactivation takes effect on a prospective basis and doesn't unwind transactions already executed.

If you believe a transaction was executed outside your configured parameters or in error, contact us at dpo@loanch.com. You have the right to request human review, explain your position, and contest the outcome. We'll investigate and respond in writing.

10.2 Other automated processing

We use automated processing for fraud detection, AML transaction monitoring, sanctions screening, and account security. This involves profiling: analysing patterns in account activity and comparing data against risk indicators and watchlists. It's not the same as Auto Invest: where a flag is raised, a member of our compliance team reviews it before any action is taken on your account.

11. How Long We Retain Personal Data

How long we keep your data depends on what it is and why we have it:

- KYC, AML, and due diligence records: at least 5 years after your account closes or the relevant transaction ends, as required by anti-money laundering law.
- Account, investment, and transaction records: for the life of your account, then as long as accounting, tax, and regulatory rules require (in some cases up to 11 years).
- Support messages and complaints: as long as needed to resolve the matter, plus a buffer for legal purposes.
- Marketing preferences: until you unsubscribe or withdraw consent. We keep suppression records after that so we don't contact you again by mistake.
- Website and technical data: in line with our Cookie Policy and internal practices.
- Legal claims and authority requests: for as long as the matter is open, including any applicable limitation periods.

When a retention period ends, we delete or anonymise the data. If a specific law sets a longer period, that takes precedence.

12. How We Share Personal Data

We share personal data only where we have a reason to: a legal obligation, contract performance, or legitimate interest. We never sell it.

12.1 Service providers

We use third parties to run our platform: hosting, KYC and AML screening, payment processing, IT support, analytics, and customer support. When they process data on our behalf, they're bound by data processing agreements that restrict what they can do with it.

12.2 Banks and payment providers

Payments, withdrawals, and account funding require us to share relevant data with the banks and payment processors handling those transactions.

12.3 Professional advisers

Our lawyers, auditors, accountants, and insurers receive data when we need advice, are managing a legal matter, or need to demonstrate regulatory compliance.

12.4 Loan originators and business partners

Running the marketplace means sharing relevant data with loan originators and other parties involved in specific transactions or service arrangements.

12.5 Your organisation

If you act on behalf of a company, we may share your data with that organisation, for example to confirm your authority or manage the account relationship.

12.6 Regulators and authorities

We share with courts, regulators, law enforcement, tax authorities, and financial intelligence units when required by law or when we need to defend ourselves in legal proceedings.

12.7 Corporate transactions

If LOANCH is involved in a merger, acquisition, or restructuring, personal data may be transferred as part of that process, subject to appropriate confidentiality arrangements.

Third parties who receive your data as independent controllers operate under their own privacy policies.

13. International Transfers

LOANCH is based in Croatia and processes most personal data within the EEA. However, our services involve loan originators and service providers operating outside

the EEA (including in Asia), which means some personal data is transferred internationally as part of how the platform works.

Where we transfer data outside the EEA, we rely on an adequacy decision by the European Commission (Article 45 GDPR), Standard Contractual Clauses (Article 46 GDPR), or, in limited cases, a derogation under Article 49 GDPR. Where the nature of the transfer requires it, we apply supplementary technical and contractual measures on top of those safeguards.

If you want to know which mechanism applies to a specific transfer involving your data, email dpo@loanch.com.

14. Cookies and Similar Technologies

We use cookies and similar tools on our website. Some are essential: without them, the site doesn't work. Others help us understand how people use it, remember your preferences, or measure the reach of our communications.

You can manage your cookie preferences through the settings banner on our website or through your browser. Switching off non-essential cookies won't break the site, but some features may work less smoothly.

For the full breakdown of which cookies we use, what they do, and how long they last, see our Cookie Policy.

15. Data Security

We protect personal data using access controls, encryption in transit and at rest, multi-factor authentication, activity logging, incident detection, vendor due diligence, and backup and recovery systems. Staff with access to personal data receive security training.

No system is completely secure, and we don't claim otherwise. What we can say is that we take security seriously and review our measures as the threat landscape changes.

16. Data Breaches

If we discover a personal data breach, we assess what happened, what data was affected, and what risk it creates for the people involved.

If the breach meets the reporting threshold under GDPR, we notify AZOP within 72 hours. If it's likely to create a high risk to your rights and freedoms, we'll notify you directly (by email or through your account) without undue delay.

17. Your Rights

Under GDPR, you have the following rights over your personal data:

- Access: ask us whether we hold data about you and get a copy of it.
- Rectification: ask us to correct inaccurate or incomplete data.
- Erasure: ask us to delete your data where the law permits.
- Restriction: ask us to pause certain processing while a dispute is resolved.
- Portability: receive your data in a machine-readable format, or ask us to send it to another provider.
- Object: object to processing based on legitimate interests, or opt out of direct marketing at any time.
- Withdraw consent: if we rely on your consent, you can withdraw it at any time without affecting what we did before.
- Automated decisions: if a significant decision about you was made purely by algorithm, you can ask for human review and contest the outcome.
- Complain: lodge a complaint with AZOP (Croatia) or any EU supervisory authority where you live or work.

These rights aren't absolute. We can refuse or limit a request where the law requires it, for example to protect AML records, comply with a legal obligation, or defend a legal claim. We'll always tell you if we're unable to act on a request and why.

18. How to Exercise Your Rights

Email dpo@loanch.com. Tell us what you're asking for and include enough information to identify your account. We may follow up to verify your identity first.

We'll respond within one month. If your request is complex, we may take up to three months in total; we'll let you know if that applies.

Exercising your rights is free. We can charge a reasonable fee or decline if a request is clearly excessive or repetitive.

Some requests we can't fully honour. Data we're legally required to keep for AML, tax, or accounting purposes can't always be deleted on request. We'll explain what we can and can't do and why.

19. Children

LOANCH is not for people under 18. If we discover we've collected data from someone under 18 without a valid legal basis, we'll delete it.

20. Changes to this Privacy Policy

We update this Policy when our services or legal obligations change. For material changes, we'll notify you in advance (by email or through your account) before the new version takes effect.

The effective date at the top of this document tells you which version you're reading.

21. Complaints and Contacting the Supervisory Authority

If something about how we handle your data concerns you, email us first at dpo@loanch.com. We'll look into it and respond.

If you're not satisfied, or prefer to go directly to the regulator, you can contact the Croatian Personal Data Protection Agency (AZOP).