Privacy Policy

1. Introduction

This Privacy Policy describes how Nimble Finance Ltd. ("Nimble", "we", "us", or the "Company") collects, uses, stores, shares, and otherwise processes personal data in connection with Nimble's website at https://www.nimble-finance.com (the "Website"), Nimble's digital platform and related online services made available from time to time (the "Platform"), and Nimble's services and business activities.

This Privacy Policy is intended to comply with applicable data protection laws, including the Protection of Privacy Law, 1981 (as amended), and, where applicable, the General Data Protection Regulation (GDPR). For the purposes of applicable data protection laws, Nimble acts as the controller of personal data processed in connection with the Website, Platform, services, and business activities described in this Privacy Policy.

Nimble primarily provides services to businesses. However, in the course of providing such services, Nimble may collect and process personal data relating to individuals associated with those businesses, including authorized signatories, representatives, shareholders, beneficial owners, directors, employees, guarantors, sole proprietors, and other individuals connected to a customer or prospective customer. References in this Privacy Policy to "you" include such individuals, where applicable.

You are not legally required to provide personal data, but without it Nimble may not be able to provide some or all services. In certain cases, providing personal data may be necessary for Nimble to comply with applicable legal, regulatory, AML, CTF, KYC, fraud prevention, or other compliance obligations.

By using the Website, Platform, or services, you acknowledge that personal data may be collected and processed as described in this Privacy Policy. Where consent is required by applicable law, Nimble will request such consent separately.

Terms not defined in this Privacy Policy have the meanings assigned to them in Nimble's Terms of Use.

2. Types of Information We Collect

When you use the Website, Platform, or services, we may collect the following types of personal data:

i. **Identification details:** Full name, ID or passport number, photo ID (including date of birth, gender, issuing authority, etc.).

ii. **Contact details:** Phone number, email address, physical address.

iii. **Financial and commercial information:** Source of funds, bank account details, payment details, transaction data, invoices, agreements, credit or financing documents, uploaded documents or files, payment history, credit limits, collateral, guarantees, financial activity profile, risk-related data, and other financial or commercial information required for onboarding, underwriting, risk assessment, or provision of the services.

iv. **Business-related personal data:** information relating to individuals associated with a business customer or prospective customer, including authorized representatives, signatories, directors, officers, shareholders, beneficial owners, guarantors, sole proprietors, employees, and contact persons. This may include identification, contact, role, ownership, authorization, and verification information.

v. **Compliance and verification information:** information required for customer due diligence, KYC, KYB, AML, sanctions screening, fraud prevention, regulatory reporting, and risk management purposes.

vi. **Website and Platform usage information:** e.g., session durations, navigation behavior, login activity, account access records, user actions, and actions taken on the Website or Platform.

vii. **Technical information:** e.g., IP address, internet provider, device type, and OS details.

viii. **Additional information:** Any data you may provide regarding yourself or third parties.

We may also process statistical or aggregated data for lawful business purposes. This type of data does not identify individuals and is not considered personal data.

Certain categories of personal data, including identification, financial, compliance, and verification information, may be considered sensitive or require enhanced protection under applicable law.

If you provide personal data about third parties, you must obtain their consent or otherwise ensure that you are legally permitted to provide such information to Nimble. You bear sole responsibility for doing so.

3. How We Collect Information

Nimble may collect personal data directly from you, automatically through your use of the Website, Platform, or services, and from third-party or publicly available sources, as described below.

Direct submission: You may provide identification, contact, financial, business, and transaction-related information through the Website, Platform, onboarding flows, document uploads, registration processes, or communications with us.

Automated collection: We may automatically collect usage and technical data through logs, cookies, and similar technologies.

Public and third-party sources: We may receive personal data, business-related information, credit indications, or credit data from third parties, including the Bank of Israel, the Capital Markets Authority, government agencies, business partners, analytics providers, credit information and business information providers, public registers, corporate registries, pledge registries, databases, identity verification providers, payment service providers, financial institutions, sanctions and watchlist screening providers, fraud prevention providers, and other permitted sources, where such information is required and permitted by applicable law for compliance, verification, risk assessment, credit assessment, underwriting, fraud prevention, or service provision purposes.

Where we receive personal data about you from a business customer, prospective customer, representative, or other third party, we process such information in accordance with this Privacy Policy and applicable law.

4. Purposes of Data Collection and Usage

Nimble collects and processes personal data only to the extent necessary for the purposes described below. Where the GDPR applies, the table also describes the legal basis on which Nimble relies for each processing activity.

Purpose	Categories of Personal Data	Legal Basis (where GDPR applies)
Providing, managing, and improving the services; executing agreements; managing customer accounts and platform access.	Identification details; contact details; business-related personal data; financial information; Website and Platform usage information.	Performance of a contract; legitimate interests.
Customer onboarding, customer due diligence, identity verification, KYC/KYB, AML, sanctions screening, fraud prevention, underwriting, risk assessment, credit assessment, transaction monitoring, regulatory reporting, and other compliance activities.	Identification details; financial information; business-related personal data; compliance and verification information; technical information.	Compliance with legal obligations; legitimate interests.
Communicating with you, responding to inquiries, providing support, and sending service-related notices through SMS, WhatsApp, email, Website notifications, or other channels.	Contact details; identification details; business-related personal data; correspondence and support information.	Performance of a contract; legitimate interests; compliance with legal obligations.
Operating, securing, maintaining, troubleshooting, and improving the Website, systems, products, and related technologies.	Technical information; Website and Platform usage information; device identifiers; logs; account and access information.	Legitimate interests; compliance with legal obligations.
Sending marketing communications, customer surveys, marketing research, promotional content, and, where applicable, personalized advertising.	Contact details; marketing preferences; Website and Platform usage information; technical information.	Consent where required by applicable law; legitimate interests where permitted.
Managing legal proceedings, enforcing agreements, responding to court orders, regulator requests, or legal claims, and protecting Nimble's rights and interests.	Identification details; contact details; financial information; business-related personal data; compliance and verification information; correspondence.	Compliance with legal obligations; legitimate interests; establishment, exercise, or defense of legal claims.
Processing information for purposes to which you have consented.	Relevant categories of personal data depending on the consented purpose.	Consent.

Nimble may use internal systems, external databases, service providers, and automated or semi-automated tools to support onboarding, verification, fraud prevention, risk assessment, credit assessment, transaction monitoring, and compliance activities.

5. Disclosure to Third Parties

Nimble may share personal data with the following categories of recipients, where necessary for the purposes described in this Privacy Policy and subject to applicable law:

Business partners, contractors, or service providers, including providers of cloud hosting, infrastructure, payment, banking, foreign exchange, identity verification, KYC/KYB, AML, sanctions screening, fraud prevention, analytics, software, support, SMS, email, and communication services. Such providers may include AU10TIX, where applicable, for identity verification, document verification, KYC/KYB, and fraud prevention purposes.

Professional advisors, including lawyers, accountants, auditors, and other consultants.

Affiliates of Nimble, where relevant, for group management, service provision, compliance, security, risk management, or other permitted business purposes, in accordance with this Privacy Policy.

Authorities, regulators, courts, law enforcement agencies, financial institutions, AML authorities, tax authorities, or other competent bodies, where required or permitted by law or necessary for compliance, reporting, investigation, or legal proceedings.

Third-party financial technology and payment service providers, including Plaid Inc. and Airwallex, where applicable, to enable users to connect financial accounts, verify account ownership, retrieve financial account information, support payment, banking, foreign exchange, digital wallet, and payment-related services, or perform KYC/KYB, AML, sanctions screening, compliance, fraud prevention, risk management, and transaction monitoring checks. Where you choose to use functionality involving such providers, you authorize Nimble and the relevant provider to access, transmit, store, and process the personal and financial information necessary to provide the relevant functionality, in accordance with this Privacy Policy and the provider’s applicable terms and privacy policy.

Third parties involved in an actual or potential corporate transaction, such as a merger, acquisition, financing, reorganization, sale of assets, or similar transaction.

Third parties for marketing or advertising purposes, subject to applicable law and your right to object or opt out where required.

Other third parties with your consent or as otherwise required or permitted by applicable law.

Certain service providers may process personal data on Nimble’s behalf, subject to appropriate contractual, confidentiality, security, and data protection obligations.

We share personal data only where necessary for the purposes described in this Privacy Policy, including service provision, compliance, risk management, fraud prevention, security, legal proceedings, or business operations.

Where relevant, Nimble may share personal data, including transaction, payment, verification, or attempted-transaction information, with financial institutions, payment service providers, fraud prevention providers, and other relevant partners to help assess, prevent, detect, investigate, or mitigate fraud, unauthorized activity, compliance risk, credit risk, financial loss, or security incidents.

Personal data may be transferred, stored, or processed outside your country of residence, including outside Israel and the EEA, by Nimble’s affiliates, service providers, business partners, or other recipients described above. Where such transfer occurs, Nimble will implement appropriate safeguards required by applicable law, such as contractual protections, data processing agreements, Standard Contractual Clauses, adequacy-based transfers, or other recognized transfer mechanisms.

6. External Sites

The Website may contain links to external websites. Clicking on such links may lead to the collection of personal data by third parties. Such third parties may process personal data in accordance with their own terms, privacy policies, and data protection practices. We have no control over external websites and bear no responsibility for them. We recommend reviewing their terms and privacy policies before use.

7. Data Security

We implement technological and organizational security measures to protect personal data under our control from accidental or intentional misuse, loss, destruction, or unauthorized access, including, as appropriate, access controls, encryption, monitoring, logging, employee access restrictions, vendor security controls, and periodic security assessments.

However, no system can be guaranteed to be completely secure or fully immune from unauthorized access, breaches, or cyber threats. If we become aware of a security incident affecting personal data, we will handle it in accordance with applicable law and our internal incident response procedures.

8. Cookies and Similar Technologies

Cookies are files stored on your device through your browser for record-keeping and technical purposes. They may help operate the Website, enable certain functionality, improve performance, support security, remember preferences, and understand how users interact with the Website.

Nimble uses cookies and similar technologies, including technologies provided by third parties, for Website operation, security, performance improvement, analytics, user experience enhancement, and, where applicable, marketing or advertising purposes. These technologies may collect technical and usage data, such as device identifiers, IP address, browser information, pages visited, time spent on the Website, referral sources, and preferences.

Some cookies are necessary for the operation and security of the Website. Other cookies, such as analytics or marketing cookies, may be used only where permitted by applicable law and, where required, subject to your consent.

You can manage or disable cookies through your browser settings. Disabling certain cookies may affect the functionality, availability, or user experience of the Website.

9. Minors

The Website is not intended for individuals under 18. We do not knowingly collect personal data from children under 18. If you are a parent or legal guardian and believe your child is using the Website or that we have collected personal data about your child, please notify us immediately. Verification of your identity may be required before we take any action.

10. Data Retention

We retain personal data for as long as necessary to fulfill the purposes for which it was collected, including providing services, maintaining business records, complying with legal, regulatory, tax, accounting, anti-money laundering, and reporting obligations, resolving disputes, and enforcing agreements.

Retention periods are determined based on the nature and sensitivity of the personal data, the purposes of processing, applicable legal and regulatory requirements, potential risks from unauthorized use or disclosure, and the period during which the data may be required for legal claims or regulatory review.

When personal data is no longer required, Nimble will delete it, anonymize it, or otherwise restrict its use, unless continued retention is required or permitted by applicable law.

11. Your Rights

Subject to applicable law, you may request to access, review, correct, or delete personal data held about you. Where applicable, you may also have the right to restrict or object to certain processing activities, withdraw consent where processing is based on consent, and receive a copy of certain personal data in a structured and commonly used format.

Requests may be submitted using the contact details below. Nimble may request information to verify your identity and will respond within the timeframes required by applicable law. Nimble may decline a request, in whole or in part, where permitted by law, including where continued retention or processing is required for legal, regulatory, contractual, security, fraud prevention, or claims-related purposes.

12. Complaints

If you have concerns regarding the way Nimble processes your personal data, you may contact us using the contact details below.

Where applicable, you may also have the right to lodge a complaint with a competent data protection authority, including the Israeli Privacy Protection Authority or, if the GDPR applies, the relevant supervisory authority in the EEA.

13. Changes to the Privacy Policy

We may update this Privacy Policy from time to time, including to reflect changes in our services, business practices, legal requirements, or data processing activities. The updated Privacy Policy will be published on the Website and will become effective upon publication, unless otherwise stated.

Where required by applicable law, or where we make material changes to the way we process personal data, we may provide additional notice through the Website, by email, or through other reasonable means.

14. Contact Information

For questions regarding this Privacy Policy or the processing of personal data by Nimble, or to exercise your rights under applicable law, please contact us at:

privacy@nimble-finance.com

Please include your full name and contact details to help us respond effectively.

Last Updated: August 16, 2026