Privacy Policy

Blokko Payments Inc. Last Updated: March 1st, 2026

Last Updated: March 1st, 2026

I. Introduction and Scope

At **Blokko Payments Inc.** ("We", the "Company" or "Blokko"), your privacy is our priority. This policy explains how we collect, use, and protect the personal data of our users in the United States, in accordance with applicable U.S. federal and state privacy laws, including the California Consumer Privacy Act ("CCPA"), the Gramm-Leach-Bliley Act ("GLBA"), and other applicable financial privacy regulations. This Privacy Policy applies to all users of our Service located in the United States, and those in the European Union/European Economic Area or other jurisdictions conducting transactions via Blokko.

We are committed to ensuring that your privacy and personal information is protected, and should we ask you to provide us certain information while using our Site (www.blokko.io)(the "Site") or our Service, you can be assured that it will only be used as stated in this policy. This Privacy Policy applies to all users of our Service located in the United States, and those in the US, European Union/European Economic Area or other jurisdictions conducting transactions via Blokko. For users in the EU/EEA, this policy complies with the General Data Protection Regulation ("GDPR").

We may revise our policy from time to time in order to better comply with new laws or changes to our Services, but we will always inform you of these changes before they affect you personally, and we will only subject your personal data to the new rules once you give us your personal consent. We require your express consent to acceptance of our Privacy Policy and any revisions thereof. If you do not consent to this privacy policy, please do not use our Services. This policy is effective as of **March 1st, 2026**.

II. Data Controller Information

Entity: Blokko Payments Inc.

Privacy Officer / Department:customerservice@blokko.io

III. Information We Collect

To provide payment services, we collect:

Registration Data: Full name, Social Security Number (SSN) or Individual Taxpayer Identification Number (ITIN), date of birth, and address.

Financial Data: Bank account details (routing number and account number), transaction history, credit card numbers (tokenized), and billing info.

Technical Data: IP address, geolocation (crucial for fraud prevention), device ID, and cookies.

Sensitive Data: Biometric data (facial recognition) for identity verification (KYC) and security. In accordance with applicable U.S. state biometric privacy laws (including the Illinois Biometric Information Privacy Act, "BIPA", and similar state laws), we treat biometric data as sensitive and require your express written consent for its processing.

We may need to eventually collect additional types of information, but we will only do so after updating our privacy policy, and only once you give us your consent. In addition, we may offer certain promotions or surveys which ask for additional categories of information, but these will be optional and we will always request your consent before offering them to you.

For all users we may request the right to collect location data and geographic data, as well as telephone numbers. This information may be necessary for us to prevent fraudulent activities, and to verify user credentials.

IV. Purposes for Processing and Legal Basis for Processing

We process your data for the following Primary Purposes, which are necessary for the service:

Compliance with Legal Obligations: Reporting to the Financial Crimes Enforcement Network (FinCEN), the Consumer Financial Protection Bureau (CFPB), the IRS, and other applicable U.S. federal and state regulators (AML/BSA compliance).

Execution of Contract: Processing payments, managing your account, and providing technical support.

Security & Fraud Prevention: Monitoring for unauthorized access and protecting the U.S. financial system.

Marketing & Analytics: Sending promotions or internal research to improve our products. You may opt-out of these secondary purposes at any time.

Additionally, we collect data for the following purposes:

- Internal record keeping;
- to improve our products and services;
- To provide, operate, and maintain our Services;
- To create and manage your account;
- To process transactions and send transaction notifications;
- To provide customer support and respond to inquiries;
- To send administrative information, updates, and security alerts;
- To enable the Service offered by the Site;

- To improve interaction between us and our users, including for better customer and tech support;
- To verify the identity of customers for fraud prevention activities;
- To comply with legal obligations and regulatory requirements

LEGAL BASIS FOR PROCESSING (GDPR)

For users in the European Union/European Economic Area, we process your personal data based on the following legal grounds under the GDPR:

Contractual Necessity

Processing is necessary for the performance of our contract with you (Article 6(1)(b) GDPR), including:

- Providing access to our Site
- Processing payments
- Delivering customer support

Legitimate Interests

Processing is necessary for our legitimate business interests (Article 6(1)(f) GDPR), including:

- Improving our Service
- Conducting analytics and research
- Fraud prevention and security
- Direct marketing (where permitted)

Legal Obligation

Processing is necessary to comply with legal obligations (Article 6(1)(c) GDPR), including:

- Tax reporting requirements
- Regulatory compliance
- Responding to lawful requests from authorities

Consent

Where required by law, we obtain your explicit consent (Article 6(1)(a) GDPR) for:

- Marketing communications
- Non-essential cookies
- Processing special categories of data (if applicable)

You have the right to withdraw consent at any time without affecting the lawfulness of processing based on consent before its withdrawal.

We currently use automatic decision making or profiling technologies that require your personal information to operate. Automatic decision making is the process of using bots, AI, or monitoring programs to make decisions which might affect your use of our services, or which might have an effect on your personal information. While registration is automatic, you will have full control over your personal information, and no automatic system will limit your access to the data, or prevent your control of the information. You further have the right to review decisions made by our automated processing systems.

V. Data Sharing

We may share your data with:

Financial Partners: Banking correspondents, card networks (Visa/Mastercard), and the ACH Network (Automated Clearing House).

Authorities: FinCEN, the IRS, and the Office of Foreign Assets Control (OFAC).

International Transfers: As our data servers are located in the United States, your information is stored and processed here. We ensure that these transfers comply with applicable U.S. and international data protection laws through appropriate data protection safeguards.

Fraud Prevention Agencies: To protect your account from unauthorized transactions.

VI. Security Measures

We maintain a robust cybersecurity posture as required by U.S. federal and state financial regulations, including the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule and applicable state data security laws, including:

Encryption of data in transit and at rest. SSL/TLS encryption for all data transmission.

Multi-factor authentication (MFA) for all sensitive operations.

Compliance with **PCI-DSS** for card data.

Independent Audits: Annual intrusion and penetration testing conducted by specialized third parties.

Cloud Governance: Ensuring all data stored in the cloud remains accessible for Central Bank inspections.

VII. Retention Period

We store your data only for as long as necessary to fulfill the purposes outlined or to comply with applicable U.S. legal requirements (5 years for financial records under IRS requirements and applicable federal recordkeeping rules).

VIII. Consent Management

In accordance with U.S. law, we ensure that you have full control over how your data is used for non-essential services.

Granular Consent: Within our application settings, you can manage permissions for specific activities, such as receiving push notifications, marketing emails, or sharing data for personalized credit offers.

Withdrawal of Consent: You may revoke your consent at any time through the "Privacy Center" in the app. Please note that withdrawing consent does not affect the legality of processing carried out prior to the withdrawal.

System Permissions: Our app may request access to your **Contacts** (to facilitate transfers), **Camera** (for KYC/biometrics), and **Location** (to prevent fraud). These can be toggled via your mobile device's operating system settings.

Consequences of Denial: If you choose not to provide consent for essential operational data (such as identity verification), we may be unable to open or maintain your account due to regulatory requirements.

IX. Fraud Prevention & ACH Monitoring

To ensure the security of our ecosystem and comply with local and federal laws, **Blokko** performs continuous monitoring of all transactions and account behaviors.

Behavioral Analysis: We use automated systems and artificial intelligence to analyze usage patterns (such as login location, transaction frequency, and typical amounts). This helps us identify "mule accounts" (accounts used by third parties to facilitate illicit activities) or unauthorized access.

Transaction Rejection & Blocking: We reserve the right to **reject payments or temporarily block accounts** if we identify a high risk of fraud or involvement in irregular activities.

Inter-Institutional Sharing: We participate in the mandatory sharing of "fraud indicators" with other financial institutions. This means if an account is flagged for fraud here, the information may be shared through a centralized system to prevent that same agent from committing crimes elsewhere in the National Financial System.

ACH Network: For ACH and instant payments, your data (Name, routing/account number) may be visible to the receiver as a security feature of the payment protocol.

Mule Account Detection. We perform real-time behavioral monitoring:

Transaction Rejection: We may automatically block transactions to or from accounts flagged in national fraud databases.

Inter-Institutional Sharing: We share "fraud indicators" with other banks to protect the financial network.

Account Closure: If an account is confirmed as a "mule account," we are legally required to terminate the relationship.

X. Biometric Data and Identity Proofing

To protect your identity and prevent the unauthorized opening of accounts by third parties (using deepfakes or stolen documents), **Blokko** uses advanced biometric verification technology during onboarding and for high-risk transactions.

Sensitive Data Processing: Facial biometrics are classified as "Sensitive Personal Data" under the applicable U.S. state biometric privacy laws (including BIPA and similar state statutes).

Liveness Detection: To ensure that the person interacting with our app is a real human being and not a pre-recorded video, deepfake, or static photo, we perform "Liveness Tests" (active or passive). This may require you to perform specific movements (e.g., blinking, turning your head) or simply capture a high-resolution selfie.

Deepfake Prevention: Our systems use AI-driven analysis to detect "injection attacks" and synthetic media. We analyze digital artifacts, skin texture, and depth signals to ensure the authenticity of the biometric capture.

Comparison and Validation: Your biometric profile is compared against the photo on your official identification document and may be cross-referenced with public or private databases to confirm your identity.

Storage and Security: Biometric templates (mathematical representations of your face) are stored with high-level encryption and are never shared with third parties for marketing purposes. This data is kept only for the duration required by applicable U.S. law for KYC records.

XI. Secured Data

We are committed to ensuring that your information is secure. In order to prevent unauthorized access to disclosure of your personal information we have put in place suitable physical, electronic, and managerial procedures to safeguard and secure the information we collect online. These include internal reviews of our data collection, storage, and processing practices and security measures, as well as physical security measures to guard against unauthorized access to systems where we store personal data.

Our security measures include:

- **Encryption**: Data transmission using SSL/TLS encryption
- **Access Controls**: Role-based access restrictions and authentication
- **Secure Storage**: Encrypted data storage and secure backup systems
- **Regular Audits**: Periodic security assessments and vulnerability testing
- **Employee Training**: Staff training on data protection and security practices
- **Incident Response**: Procedures for detecting and responding to security breaches

XII. Data Breach Notification (GDPR)

In the event of a personal data breach that is likely to result in a risk to your rights and freedoms, we will:

- Notify the relevant supervisory authority within **72 hours** of becoming aware of the breach (GDPR Article 33)
- Notify affected individuals without undue delay if the breach is likely to result in a high risk (GDPR Article 34)
- Document all data breaches, including facts, effects, and remedial action taken

Please note that the Internet is an open system and we cannot provide absolute assurances that your data or communications cannot be intercepted or viewed by third parties. In the event that a data breach occurs for any reason, we will immediately inform you if any of your personal information has been compromised.

XIII. How we use cookies?

A. A cookie is a small file which asks permission to be placed on your computer or mobile device's hard drive. Once you agree, the file is added and the cookie helps analyze web traffic or lets you know when you visit a particular site. Cookies allow web applications to respond to you as an individual. The Service can tailor its operations to your needs, likes, and dislikes by gathering and remembering information about your preferences.

B. We use traffic log cookies to identify which pages are being used. This allows us to analyze data about Site traffic and visitor trends in order to improve the Service based on our users' needs. We only use this information for statistical analysis purposes and the information is only temporarily stored. Once we are done analyzing the statistical information the data is removed from our system.

C. Overall, cookies help us provide our users with a better website experience, by enabling us to monitor which pages you find useful and which you do not. A cookie in no way gives us access to your computer, phone, or other hardware or any information about you, other than the data you choose to share with us.

D. You can choose to accept or decline cookies. Upon accessing our Site for the first time you will be given the option to enable cookies. If you do not enable cookies, we will not download a cookie into your browser for any purpose, but your usage of the Site may be limited. Once you create a user profile you may additionally disable

or enable cookies at any time through the appropriate option on the user profile tab. Please be aware that declining cookies may prevent you from taking full advantage of the Site. Cookies can also enable us to track and target the interests of our users to enhance the experience on our Site. Cookies do not record any personal information, and the usage of a cookie will in no way allow us or any other person or company to access your personal information without your express consent.

XIV. Links to Third Party Websites

Our Site may from time to time contain links to enable you to visit non-affiliated third-party websites. However, by clicking on these third-party links, you will effectively be leaving our network, and we will be unable to assure the protection of any data you submit to any third-party site. Note that we do not have any control over the content contained in any third-party website featured on our Site. Please be aware that any information you submit on these sites may be subjected to other rules, and that you should review the third party's privacy policy prior to submitting any information. You should exercise caution in your use of any third-party site, and we urge you to take care before submitting any information.

XV. Controlling your personal information

A. We will not sell or transfer your personal information to third parties unless we are required to by a court or government order. We do not share your information with other users, except payment, bank partners, banking and card processing partners, cryptocurrency exchange partners (for crypto currency payments), technology providers and other parties as set forth in Section V above, for purposes of processing a payment. We may from time to time request that you allow us to share your personal information with other companies or partners for the purpose of enhancing our products and services, or to introduce you to services or products that you may find beneficial. However, we will never share any personal information without your consent, and if you decline to allow us to share your personal information it will not negatively impact your user experience. We currently don't share your information with any other company or person other than sharing payment, bank and personal information as needed or required, with the parties set forth in Section V above, so that purchases can be processed and delivered, but if we ever do, we will first give you the name and contact information for the company or person. We will not offer to share your information with any third party which does not comply with the minimum protections of US and EU privacy regulations.

B. Note that when you voluntarily disclose personal information online in a public forum or in private communications with other users (for example, through email, chatrooms, message boards, or social media) such information can be collected and used by others without our ability to control it. Therefore, if you post personal information online that is accessible to the public, it is possible that your information will not be protected and may be accessed by the general public. You may receive unsolicited messages from other parties in return, or may be subject to violations of privacy. Some of our services may offer the option to show your name, phone number and e-mail address. If you decide to show your name, phone number and e-mail address, in some instances it may be available for others over the Internet.

C. Please be aware that in the event that you to make disclosures of your identity and image publicly, we cannot absolutely guarantee that a third party will not gain access to such information illicitly or accidentally; however, we will not publish any of your personal information, and protect such information with the highest care.

D. The Company may release personal information to third parties if it is required or compelled to do so to (i) satisfy any applicable law, regulation, legal process, or enforceable governmental request like a court order or order by a government; (ii) enforce applicable Terms of Service, including investigation of potential violations thereof, such as preventing disruptive behavior; (iii) detect, prevent or otherwise address fraud, security, or technical issues, such as scammers or hackers; or (iv) protect against imminent harm to the rights, property, or safety of the Company, its users, or the public as required or permitted by law. Such as to investigate threats of violence or harm to our users, employees, or any other person.

E. Please note that we operate in the United States and all of our data servers and all saved data are located in the United States. If you are a non-resident of the United States, please be aware that your personal data will be saved in these U.S. servers and will be subject to U.S. laws and jurisdiction, except where applicable EU/EEA or other international data protection laws (including the GDPR) may apply.

XVI. Disclaimer

Except as provided elsewhere in our Privacy Policy, we will never provide your information to a third party without your express consent, but if you have consented to us sharing this information we cannot be held responsible for how these other parties use your information. While we safeguard your information and place certain restrictions on our users and other parties with respect to the dissemination of your contact information, we have no control over what users or third parties do with data you have consented to share. In the event that such data is misused by such user or third party, we will not be responsible for such misuse or unauthorized dissemination of your personal information, and shall not be liable in any way for the actions of any person or company which may receive your contact information.

XVII. International Data Transfers (GDPR)

We are based in the United States. If you are accessing our Service from other regions with data protection laws, please note that your personal data will be transferred to, stored, and processed in the United States. The United States may not provide the same level of data protection as your home jurisdiction. However, we take appropriate safeguards to ensure your personal data remains protected in accordance with this Privacy Policy and applicable law.

A. **Transfer Mechanisms**

For EU/EEA users, we rely on the following mechanisms for international data transfers:

- **Standard Contractual Clauses (SCCs)**: We use European Commission-approved Standard Contractual Clauses with our service providers

• **Adequacy Decisions**: Where applicable, we rely on European Commission adequacy decisions
• **Your Explicit Consent**: Where required, we obtain your explicit consent for data transfers

B. Your Rights Regarding Transfers

You have the right to obtain information about the safeguards we have in place for international transfers and to obtain a copy of the relevant transfer mechanisms by contacting us at customerservice@blokko.io.

XVIII. Data Retention

We retain your personal information for as long as necessary to fulfill the purposes outlined in this Privacy Policy, unless a longer retention period is required or permitted by law.

A. Retention Periods

• **Active Account Data**: Retained for the duration of your account and Service usage
• **Backup Data**: Retained for **five (5) years** in our backup systems for disaster recovery and business continuity purposes
• **Payment Information**: Retained as required by tax and accounting regulations (5 years)
• **Marketing Data**: Retained until you unsubscribe or withdraw consent
• **Legal Compliance**: Retained as required by applicable laws and regulations

B. Deletion After Retention Period

After the applicable retention period expires, we will:

• Securely delete or anonymize your personal data
• Remove identifiable information from backup systems on the next backup cycle
• Ensure data cannot be reconstructed or re-identified

XIX. Your Rights and Choices

A. Rights for All Users

You have the following rights regarding your personal information:

• **Access**: Request access to the personal information we hold about you
• **Correction**: Request correction of inaccurate or incomplete information
• **Deletion**: Request deletion of your personal information (subject to legal retention requirements)
• **Opt-Out**: Opt-out of marketing communications at any time
• **Cookie Control**: Manage cookie preferences through your browser settings

B. Additional Rights for EU/EEA Users (GDPR)

If you are located in the European Union or European Economic Area, you have additional rights under the GDPR:

Right to Access (Article 15)

You have the right to obtain confirmation of whether we process your personal data and to request a copy of that data.

Right to Rectification (Article 16)

You have the right to request correction of inaccurate personal data and completion of incomplete data.

Right to Erasure / "Right to be Forgotten" (Article 17)

You have the right to request deletion of your personal data when:

- The data is no longer necessary for the purposes collected
- You withdraw consent (where processing is based on consent)
- You object to processing and there are no overriding legitimate grounds
- The data has been unlawfully processed
- Deletion is required for legal compliance

Please note: Due to our five-year backup retention policy, complete deletion from all backup systems may take up to five years. However, your data will be anonymized or flagged for deletion immediately upon request.

Right to Restriction of Processing (Article 18)

You have the right to request restriction of processing when:

- You contest the accuracy of the data
- Processing is unlawful but you oppose erasure
- We no longer need the data, but you need it for legal claims
- You have objected to processing pending verification

Right to Data Portability (Article 20)

You have the right to receive your personal data in a structured, commonly used, and machine-readable format and to transmit that data to another controller.

Right to Object (Article 21)

You have the right to object to:

- Processing based on legitimate interests
- Direct marketing (including profiling)
- Processing for scientific, historical, or statistical purposes

Right Not to Be Subject to Automated Decision-Making (Article 22)

You have the right not to be subject to decisions based solely on automated processing, including profiling, which produces legal or similarly significant effects.

Right to Withdraw Consent

Where processing is based on consent, you have the right to withdraw consent at any time without affecting the lawfulness of processing before withdrawal.

Right to Lodge a Complaint

You have the right to lodge a complaint with a supervisory authority, particularly in the EU Member State of your habitual residence, place of work, or place of alleged infringement.

C. How to Exercise Your Rights

To exercise any of these rights, please contact us at:

Email: customerservice@blokko.io

We will respond to your request within **45 days** (or one month for GDPR requests). If we need additional time, we will notify you of the reason and extension period.

XX. Children's Privacy

Our Service is not directed to children under the age of 13 (or 16 in the EU/EEA). We do not knowingly collect personal information from children under these ages. If you are a parent or guardian and believe your child has provided us with personal information, please contact us at customerservice@blokko.io. If we discover that we have collected personal information from a child under the applicable age without parental consent, we will delete that information immediately.

XXI. California Privacy Rights (CCPA)

If you are a California resident, you have specific rights under the California Consumer Privacy Act (CCPA):

A. Right to Know

You have the right to request disclosure of:

- Categories of personal information collected
- Categories of sources from which information is collected
- Business or commercial purpose for collecting information
- Categories of third parties with whom we share information
- Specific pieces of personal information collected

B. Right to Delete

You have the right to request deletion of personal information we have collected from you, subject to certain exceptions.

C. Right to Opt-Out of Sale

We do not sell your personal information. However, you have the right to opt-out if we ever engage in such practices in the future.

D. Right to Non-Discrimination

You have the right not to receive discriminatory treatment for exercising your CCPA rights.

E. Exercising CCPA Rights

To exercise your CCPA rights, contact us at customerservice@blokko.io. We will verify your identity before processing your request and respond within 45 days.

XXII. Changes to Our Privacy Policy:

We reserve the right to make changes to our Privacy Policy from time to time and to remain compliant with applicable U.S. federal and state law. If we plan to make significant changes to any of our privacy policies or practices with respect to how we use personally identifiable information, we will require that you read and agree to our new policy prior to using any of the Site's services. We will notify you of any material changes by:

- Posting the new Privacy Policy on this page
- Updating the "Last Updated" date
- Sending an email notification (for significant changes)
- Providing in-app notifications

You must expressly consent to acceptance of our new Terms and Conditions in the event that we update the same. If you do not agree to the revised policy, please discontinue use of our Service. For EU/EEA users, where required by law, we will obtain your explicit consent before implementing changes that materially affect how we process your personal data.

Our privacy policy is current as of **March 1st, 2026**.

This Privacy Policy should be read in conjunction with our Terms and Conditions. In the event of a discrepancy between our Privacy Policy and our Terms and Conditions, this Privacy Policy will govern. If you feel that we are not abiding by this Privacy Policy or our Terms and Conditions, you should contact us via email immediately at customerservice@blokko.io.

Questions

Questions regarding our Terms and Conditions, our Privacy Policy or other policies can be directed to our support staff by emailing customerservice@blokko.io.

EU Representative (if applicable)

If required under GDPR Article 27, we will appoint an EU representative. Contact details will be provided here when applicable.

Data Protection Officer

For data protection inquiries, you may contact our designated privacy contact at customerservice@blokko.io.

Supervisory Authority (EU/EEA Users)

If you are located in the EU/EEA and believe we have not adequately addressed your concerns, you have the right to lodge a complaint with your local data protection supervisory authority. A list of EU supervisory authorities can be found at: https://edpb.europa.eu/about-edpb/board/members_en