Netlok Privacy Policy

Effective Date: May 8, 2026

Welcome to Netlok! We are committed to protecting your privacy and helping you understand your rights. This policy explains how we collect, use, share, and protect your personal information. If you have questions, email us at photoloksupport@netlok.com.

Executive Summary

What We Register	Why We Register It	Your Key Rights
Name, email, phone, images	To provide and secure services	Access, correct, delete, limit use, portability
Device & usage info	Improve and protect services	Opt-out of marketing, non-discrimination
Payment info (via processor)	Process transactions	California: Additional CCPA/CPRA rights including ADMT opt-out and risk assessment disclosures

1. Scope

This policy applies when you:

- Visit netlok.com
- Use Photolok® (our image-based authentication software)
- Interact with us (sales, marketing, support, events)

2. Key Definitions

- Personal Information: Data that identifies or relates to you or your household
- Photolok: Our image-based authentication software
- Services: Our website, Photolok, and related offerings
- Data Controller: Netlok, LLC (we determine how and why personal information is processed)
- Register: We do not collect personal information. We register information that you provide which is necessary to use Photolok. If you cancel your subscription, opt-out and/or request that your account be deleted, we delete your information from our database to meet current regulations.

3. Information We Register

Information You Provide

Account Information:

- Name, email address, mobile number
- Account security information and credentials
- Profile information and preferences

Payment Information:

- Credit/debit card details (processed securely by third-party processors)
- Billing address and transaction history
- We do not store payment card numbers

Communication & Support:

- Messages, emails, and chat communications
- Survey responses and feedback
- Support ticket information

Images:

- Images you chose from Photolok's image library for authentication

Information Registered Automatically

Device & Technical Information:

- IP address, browser type, device identifiers
- Operating system, device model, mobile carrier
- Screen resolution and device capabilities

Usage & Activity Data:

- Pages visited, features used, time spent
- Click patterns, navigation paths
- Search queries and interactions

Location Information:

- General geographic location (city/region level)
- Time zone information
- We do not collect precise GPS coordinates

Tracking Technologies:

- Session preferences and settings
- Usage analytics and performance metrics
- Security and fraud prevention data

4. Detailed Data Categories (CCPA Compliance)

Category	Specific Data	Sources	Business Purpose
Identifiers	Name, email, phone, IP address, device ID	Direct from you, automatic collection	Account management, authentication
Commercial	Transaction history,	You, payment	Billing, fraud prevention

Information	payment methods	processors	
Internet Activity	Browsing history, search queries, clicks	Automatic collection	Service improvement, analytics
Geolocation	City, region, time zone	Automatic collection	Localization, security
Professional Information	Company (if provided)	Direct from you	Business services, support
Sensitive Personal Information (Under 16)	Personal information of users under 16, if any	Direct from you, automatic collection	Enhanced protection under CCPA/CPRA

5. How We Use Your Information

Service Delivery

- Create and manage your account
- Provide customer support and technical assistance
- Process transactions and billing
- Authenticate your identity through Photolok
- Deliver and personalize our services

Security & Fraud Prevention

- Detect and prevent fraudulent activity
- Monitor for security threats and vulnerabilities
- Enforce our terms of service
- Protect our rights, property, and safety

Communication

- Send service notifications and updates
- Provide customer support responses
- Marketing communications (with your consent)
- Important policy or security announcements

Business Operations

- Improve and optimize our services
- Conduct analytics and research
- Comply with legal obligations
- Develop new features and products

Artificial Intelligence and Machine Learning

We do not use your personal information, images, or authentication data to train, fine-tune, or otherwise develop any artificial intelligence or machine learning models. Your data is used solely to provide and improve the Netlok services you have subscribed to.

Legal Basis for Processing

- Consent: Marketing communications
- Contract Performance: Service delivery, account management
- Legitimate Interests: Security, fraud prevention, service improvement
- Legal Compliance: Regulatory requirements, legal obligations

6. Information Sharing

We Do Not Sell Personal Information

We do not and will not sell your personal information to third parties.

We Do Not Use Your Data to Train AI Models

We do not share, license, or otherwise transfer your personal information to any third party for the purpose of training artificial intelligence or large language models.

When We Share Information

Service Providers (Data Processors):

- Payment processors (CardConnect)
- Cloud storage providers (AWS, Google Cloud, Microsoft Cloud)
- Analytics providers (e.g., Google Analytics, Fingerprint.com, Salesforce)
- Customer support platforms
- Bound by strict confidentiality agreements where appropriate

Legal Requirements:

- Court orders, subpoenas, or legal process
- Law enforcement requests with proper authorization
- Protection of rights, property, or safety
- Compliance with applicable laws and regulations

Business Transfers:

- Mergers, acquisitions, or asset sales
- Corporate restructuring or bankruptcy
- Privacy protections maintained in all transfers

Master Contract Accounts:

- Account administrators as specified in enterprise agreements
- Authorized personnel within customer organizations
- Limited to account management and billing information

Emergency Situations:

- Imminent threats to safety or security
- Prevention of fraud or illegal activity

- Protection of our systems and infrastructure

Third-Party Service Providers

Key Partners:

- Payment Processing: CardConnect
- Cloud Infrastructure: Amazon Web Services, Google Cloud Platform, Microsoft Cloud
- Analytics: Google Analytics, Fingerprint.com, Salesforce Analytics
- Support: Salesforce, AT&T
- Security: Cloudflare, security monitoring services

For a complete list of current service providers, contact us at photoloksupport@netlok.com

7. Data Retention

Data Type	Retention Period	Deletion Method
Account Data	60 days after account closure	Secure deletion
Payment Data	Per processor requirements (typically 7 years)	Processor deletion
Authentication Logs	12 months	Automated deletion
Marketing Data	Until opt-out or 3 years of inactivity	Secure deletion
Support Communications	3 years after resolution	Secure deletion
ADMT/Risk Assessment Records	5 years after completion or duration of processing, whichever is later	Secure deletion

Retention Criteria:

- Legal and regulatory requirements
- Business necessity and legitimate interests
- Contract performance obligations
- User consent and preferences

Secure Deletion:

- Cryptographic erasure for encrypted data
- Multi-pass overwriting for unencrypted data
- Physical destruction of storage media when necessary
- Verification of complete data removal

8. Data Security

Technical Safeguards

- Encryption: AES-256 encryption at rest, TLS 1.3 in transit
- Access Controls: Multi-factor authentication, role-based access
- Network Security: Firewalls, intrusion detection systems
- Monitoring: 24/7 security monitoring and incident response

Organizational Safeguards

- Employee Training: Regular privacy and security training
- Background Checks: Security clearance for personnel with data access
- Incident Response: Comprehensive breach response procedures
- Audits: Regular security assessments and penetration testing

Your Security Responsibilities

- Keep your Photolok images confidential and secure
- Report suspicious activity immediately
- Regularly review your account settings

Important: No system is 100% secure. While we implement industry-standard protections, you use our services at your own risk.

9. Data Breach Notification

Our Commitment

- Detection: Continuous monitoring for potential breaches
- Response: Immediate containment and investigation
- Notification: Prompt communication to affected users
- Recovery: Comprehensive remediation and improvement

Notification Timeline

- Regulatory Authorities: Within 72 hours of discovery
- Affected Users: Within 72 hours unless disclosure would compromise security
- Public Disclosure: As required by law or if widespread impact

What We'll Tell You

- Nature and scope of the breach
- Types of information involved
- Steps we've taken to address the issue
- Actions you can take to protect yourself
- Contact information for questions

10. Your Privacy Rights

All Users

Access Rights:

- Know what personal information we collect and use
- Understand how we share and protect your data

- Receive copies of your personal information

Correction Rights:

- Update or correct inaccurate information
- Add missing information to your profile
- Verify the accuracy of your data

Deletion Rights:

- Request deletion of your personal information
- Close your account and remove associated data
- Note: Some data may be retained for legal compliance

Portability Rights:

- Receive your registration data in a structured, machine-readable format
- Transfer your registration data to another service provider
- Export your account information except for Photolok proprietary images

Opt-Out Rights:

- Unsubscribe from marketing communications
- Disable non-essential cookies
- Limit data collection where possible

California Residents (CCPA/CPRA)

Enhanced Rights:

- Right to Know: Detailed information about data practices
- Right to Delete: Request deletion with limited exceptions
- Right to Correct: Fix inaccurate personal information
- Right to Opt-Out: Prevent sale/sharing (we don't sell data)
- Right to Limit: Restrict use of sensitive personal information
- Right to Non-Discrimination: No penalties for exercising rights

Automated Decision-Making Technology (ADMT) Rights:

Photolok's authentication system uses metadata processing to assist in identity verification. Because human review remains integral to all authentication decisions, Photolok's system does not substantially replace human decision-making as defined under the CCPA ADMT regulations. Accordingly, the mandatory ADMT opt-out regime does not currently apply to Photolok's core authentication function.

However, as a matter of transparency, California residents may request:

- A description of how Photolok's metadata-based authentication works
- Human review of any authentication decision that affects them
- Escalation to a senior Netlok representative if they believe an authentication outcome was incorrect

To make any of the above requests, contact us via:

- Email: photolokadmin@netlok.com
- Phone: 805-717-9898

Privacy Risk Assessments:

Netlok is currently conducting privacy risk assessments for processing activities that may present significant risk to consumer privacy, as required under the 2026 CCPA regulations. These assessments cover our use of analytics services, authentication processing, and data sharing with third-party processors. Initial assessments are underway and will be completed in accordance with regulatory timelines.

Cybersecurity Audits:

Netlok does not currently meet the revenue or data volume thresholds that trigger mandatory annual cybersecurity audits under the 2026 CCPA regulations. We nonetheless conduct regular voluntary security assessments and penetration testing as described in Section 8.

Sensitive Personal Information:

- Precise geolocation not collected
- Account security information protected with enhanced controls
- Personal information of users under 16 is treated as sensitive personal information under CCPA/CPRA

Other State Privacy Rights

Netlok recognizes the privacy rights of residents of all U.S. states that have enacted comprehensive consumer privacy legislation. As of the effective date of this policy, this includes residents of the following states (in addition to California):

- Virginia (VCDPA), Colorado (CPA), Connecticut (CTDPA)
- Delaware (DPDPA), Iowa (ICDPA), Minnesota (MCDPA), Nebraska (NCDPA)
- New Hampshire, New Jersey, Tennessee, Maryland (MODPA)
- Indiana (INCDPA), Kentucky (KCDPA), Rhode Island (RIDTPPA)
- And any additional state enacting comprehensive privacy legislation after the effective date of this policy

Residents of these states generally have the following rights, subject to applicable law:

- Access, correction, and deletion of personal data
- Opt-out of targeted advertising and profiling
- Data portability
- Appeals process for denied requests
- Non-discrimination for exercising privacy rights

Connecticut Residents — Additional Rights (Effective August 1, 2026):

Connecticut residents have expanded profiling rights under 2025 amendments to the CTDPA, including:

- Right to opt-out of any automated decision producing legal or similarly significant effects
- Right to contest profiling decisions and receive a written explanation

- Right to know whether your personal data is used to train large language models (it is not — see Section 5)

Maryland Residents (MODPA):

The Maryland Online Data Privacy Act requires that Netlok limit the collection and processing of personal information to what is reasonably necessary and proportionate to provide the services you have requested. Maryland residents may request a review of what data is registered about them and why.

How to Exercise Your Rights

Email: photolokadmin@netlok.com

Phone: 805-717-9898

Mail: Netlok, LLC, 1171 Crestline Dr, Santa Barbara, CA 93105

Identity Verification:

- We may request additional information to verify your identity
- Authorized agents must provide written authorization
- Response time: 45 days (extendable to 90 days for complex requests)

11. Automated Decision-Making

Authentication Decisions

Photolok processes metadata associated with your account to assist in identity verification. This metadata-based processing supports, but does not replace, human review in authentication decisions. Human personnel review authentication outcomes, particularly in cases of access denial or suspected anomalies.

Account Security

- Automated fraud detection and prevention
- Suspicious activity monitoring
- Account lockout procedures for security

Your Rights

- Request human review of any authentication or security decision
- Understand the metadata factors used in authentication processing
- Challenge decisions that affect you adversely
- Receive a plain-language explanation of how a decision was reached

How to Request Human Review

If you wish to request human-only review of any authentication decision, you may do so through either of the following methods:

- Email: photolokadmin@netlok.com
- Phone: 805-717-9898

Requests will be processed and a human review initiated within 5 business days.

Appeal Process

- Contact support with your concern
- Provide relevant details and context
- Human review within 5 business days
- Written explanation of decision
- Escalation to management if unresolved

12. International Data Transfers

Cross-Border Processing

- Your data may be processed in the United States
- We use appropriate safeguards for international transfers
- Standard contractual clauses with international partners
- Adequacy decisions where applicable

Transfer Safeguards

- Encryption: All data encrypted during transfer
- Contracts: Privacy clauses with all international partners
- Monitoring: Regular compliance assessments
- Rights: Your privacy rights remain protected globally

U.S. Department of Justice Data Security Program

The U.S. Department of Justice's Data Security Program (DSP), which took effect on April 8, 2025, establishes restrictions on the transfer of Americans' sensitive personal data to certain countries of concern and covered persons. Netlok complies fully with the DSP.

As confirmed through our vendor review:

- Netlok does not transfer or provide access to personal data to any vendors, employees, cloud infrastructure components, or subprocessors located in or controlled by countries of concern (China including Hong Kong and Macau, Cuba, Iran, North Korea, Russia, and Venezuela)
- All vendor and third-party processor agreements include contractual safeguards preventing onward transfer of personal data to countries of concern
- Netlok monitors its data flows and vendor relationships on an ongoing basis to ensure continued compliance with the DSP

13. Children's Privacy

Under 13 (COPPA Compliance)

- Services not intended for children under 13
- We do not knowingly register information from children under 13
- If we learn we have collected such information, we delete it immediately
- Parents can contact us to request deletion of their child's information

Users Under 16

Under CCPA/CPRA, personal information of consumers under the age of 16 is classified as sensitive personal information and is entitled to enhanced protections. Netlok's services are not directed at or intended for users under 16. We do not knowingly register personal information from users under 16.

If we become aware that we have registered personal information from a user under 16, we will:

- Delete the information promptly from our systems
- Apply enhanced access controls consistent with sensitive personal information standards in the interim
- Notify the parent or guardian if contact information is available

California Minors (Under 18)

- Registered users under 18 can request removal of posted content
- Contact photoloksupport@netlok.com for assistance
- We cannot guarantee complete removal from all systems
- Some content may be retained for legal compliance

Parental Controls

- Parents can review and delete their child's information
- Account closure available upon parental request
- Educational resources available for online safety

14. Changes to This Policy

Update Process

- Material changes require 30 days advance notice
- Notice provided via email to registered users
- Prominent website notification for significant changes
- Master Contract account administrators notified separately

Continued Use

- Continued use of services after changes indicates acceptance
- Right to close account if you disagree with changes

Change Log

- May 8, 2026: Comprehensive update incorporating CCPA/CPRA ADMT rights and risk assessment disclosures; DOJ Data Security Program compliance; expansion of state privacy rights coverage; under-16 data classification as sensitive personal information; Connecticut expanded profiling rights; Maryland MODPA data minimization standard; AI/ML training non-use disclosure; explicit ADMT opt-out mechanisms; and ADMT/Risk Assessment record retention period.
- July 16, 2025: Comprehensive update for enhanced compliance and transparency
- Previous versions: Available upon request

15. Contact Information

General Inquiries

Email: photoloksupport@netlok.com

Phone: 805-717-9898

Hours: Monday–Friday, 9 AM – 6 PM PST

Privacy Requests (including ADMT & Rights Requests)

Email: photolokadmin@netlok.com

Phone: 805-717-9898

California Residents

Email: photoloksupport@netlok.com

Phone: 805-717-9898

Mailing Address

Netlok, LLC

1171 Crestline Dr

Santa Barbara, CA 93105, USA

16. Complaint Process

Internal Resolution

- Contact our privacy team with your concern
- Detailed investigation within 30 days
- Written response with resolution or explanation
- Appeal process if unsatisfied with response

External Authorities

California Residents:

- California Attorney General: oag.ca.gov/contact
- California Privacy Protection Agency: cppa.ca.gov

Federal Complaints:

- Federal Trade Commission: ftc.gov/complaint
- Consumer Financial Protection Bureau: consumerfinance.gov/complaint

State Privacy Authorities:

Residents of states with comprehensive privacy laws may also file complaints with their state's Attorney General or designated privacy enforcement authority.

International Users:

- Your local data protection authority
- EU residents: edpb.europa.eu

17. Glossary

- Automated Decision-Making Technology (ADMT): Any technology that processes personal information and uses computation to replace or substantially replace human decision-making, as defined under the California Consumer Privacy Act regulations effective January 1, 2026
- Cookies: Small files stored on your device to remember preferences
- Countries of Concern: As defined under the DOJ Data Security Program: China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela
- Data Controller: The entity that determines how and why personal data is processed
- Data Processor: The entity that processes personal data on behalf of the controller
- Data Security Program (DSP): The U.S. Department of Justice regulatory framework, effective April 8, 2025, governing transfers of Americans' sensitive personal data to countries of concern or covered persons
- Encryption: Technology that scrambles data to protect it from unauthorized access
- Personal Information: Registered information that identifies or relates to an individual and their Photolok account
- Pseudonymization: Processing data so it can no longer be attributed to a specific person without additional information

Thank you for trusting Netlok with your privacy. We are committed to protecting your personal information and respecting your privacy rights. This policy reflects our dedication to transparency, security, and your control over your personal data.

Last updated: May 8, 2026