PRIVACY POLICY OF IMAGIPORTAL INC.

Effective Date: January 17, 2026

PREAMBLE AND GOVERNANCE FRAMEWORK

This Privacy Policy ("Policy") constitutes a comprehensive, binding instrument governing the collection, processing, utilization, retention, and safeguarding of information submitted to or generated through the proprietary digital platform denominated ImagiPortal ("Platform") and all ancillary services provided by ImagiPortal Inc., a Delaware corporation ("Company," "we," "us," "our"). This Policy operates in conjunction with and as an integral component of the Terms of Service, constituting a unified binding agreement. By accessing, utilizing, or maintaining access to the Platform in any capacity whatsoever—whether through web-based interfaces, mobile applications, application programming interfaces ("APIs"), or any derivative technological implementation—users ("User," "you," "your") shall be deemed to have affirmatively acknowledged, comprehended, and unconditionally consented to all terms, conditions, and methodologies delineated herein. Failure to accept this Policy in its entirety shall irrevocably preclude User from accessing, utilizing, or maintaining engagement with the Platform.

This Policy reflects the Company's comprehensive compliance framework with respect to the General Data Protection Regulation ("GDPR") as codified in Regulation (EU) 2016/679, the California Consumer Privacy Act ("CCPA") as set forth in California Civil Code § 1798.100 et seq., the Children's Online Privacy Protection Act ("COPPA") as established in 15 U.S.C. § 6501 et seq., the Health Insurance Portability and Accountability Act ("HIPAA") to the extent applicable, and all analogous state and federal statutory regimes governing personal data, biometric information, and digital privacy architecture.

1. CATEGORICAL DESCRIPTION OF INFORMATION COLLECTED

1.1 Voluntarily Submitted Information

(a) Account Establishment Data

Upon the creation of an account, User affirmatively submits the following categories of personally identifiable information ("PII"):

- Governmental surname and forename
- Valid electronic mail address
- Unique username designator
- Secured password authentication credential
- Billing address and associated postal identifier
- Telecommunications contact number (mobile and/or residential)
- Date of birth and age verification documentation (including government-issued photographic identification in certain jurisdictions)
- Citizenship or residency classification
- Any supplementary information User elects to provide

The Company shall not be held liable for inaccuracies, incompleteness, or deceptions contained within such voluntarily submitted information. User shall bear sole and absolute responsibility for maintaining current, accurate, and truthful account information and shall indemnify the Company against any claims arising from User's misrepresentation.

(b) User-Generated Content and Proprietary Submissions

This encompasses all content created, uploaded, transmitted, or otherwise submitted to the Platform, including but not limited to:

- AI persona configurations and architectural specifications
- Textual prompts, conversational exchanges, and linguistic inputs
- Photographic images, video recordings, and multimedia files
- Voice recordings and acoustic data samples
- Biographical information, preferences, and personality attributes incorporated into AI personas
- Derivative works, modifications, and adaptations
- Communications with other Users, support personnel, and Company representatives

User explicitly warrants and represents that all submitted User-Generated Content does not violate third-party intellectual property rights, does not infringe trademark registrations, does not constitute defamatory material, and complies with all applicable statutory frameworks and regulatory regimes.

(c) Payment and Commercial Data

Through engagement with third-party payment processors and financial services providers, the Company may receive or process:

- Credit card identifiers (last four digits only; full payment card information is neither stored nor processed by Company infrastructure)
- Debit card details
- Digital payment platform credentials (PayPal, Apple Pay, Google Pay, cryptocurrency wallet addresses)
- Billing transactional history
- Subscription tier designations and renewal schedules
- Promotional discount codes and redemption records

The Company explicitly disclaims any responsibility for the security, confidentiality, or integrity of full payment card information, such responsibility remaining with certified third-party Payment Card Industry Data Security Standard (PCI DSS) Level 1-compliant processors.

(d) Communicative and Supportive Submissions

Information voluntarily provided through customer support interactions, including email correspondence, telephonic communications, in-platform messaging systems, and helpdesk submission forms.

1.2 Automatically Collected Technical and Behavioral Data

(a) Usage Telemetry and Interaction Analytics

The Company employs automated data collection mechanisms to capture comprehensive information regarding User interaction patterns, including:

- Platform features accessed and frequency of utilization

- Persona creation and modification patterns
- Chat history length and linguistic complexity measurements
- Generated content parameters and computational intensity
- Session duration and temporal engagement metrics
- Navigation pathway sequences through application architecture
- Feature abandonment rates and conversion funnel data
- Error logs and exception event records
- Crash report data and performance degradation events
- Timestamp and temporal sequence data associated with all activities

(b) Device-Level and TechnicalInfrastructure Data

Automated collection mechanisms capture technical specifications of User-operated devices:

- Internet Protocol (IPv4 and IPv6) addresses with geolocation inference
- Unique device identifiers, including but not limited to: International Mobile Equipment Identity (IMEI), Media Access Control (MAC) addresses, Android Advertising Identifier (AAID), Identifier for Advertisers (IDFA)
- Operating system version and build identifier
- Browser application identifier and version
- Device manufacturer and model specification
- Screen resolution and display characteristics
- System memory and storage capacity metrics
- Central processing unit (CPU) architecture and specifications

(c) Cookie and Session Persistence Technologies

The Company implements persistent, non-persistent, first-party, and third-party cookie technologies, including:

- Session-authenticated cookies maintaining User login persistence
- Functionality cookies enabling platform feature operation
- Preference cookies recording User-selected settings and configurations
- Analytics cookies facilitating aggregate usage pattern analysis
- Retargeting cookies enabling contextual advertising personalization
- Security cookies implementing fraud detection and malicious activity prevention

User acknowledges that disabling cookie functionality may substantially degrade Platform utility and accessibility.

(d) Biometric and Facial Recognition Data

To the extent User uploads photographic images containing facial features, the Company may process:

- Facial geometry measurements and mathematical vector representations
- Facial feature point mappings and spatial coordinates
- Iris and sclera coloration characteristics
- Facial symmetry measurements and proportion calculations
- Age estimation algorithmic outputs (derived through machine learning inference, not stored)
- Ethnicity classification probabilities (derived through algorithmic processing)
- Emotional expression recognition outputs

- Anti-spoofing liveness detection metrics

Critical Disclosure: Facial recognition data constitutes "special category personal data" under GDPR Article 9 and receives heightened statutory protection. Such data is processed solely for: (i) AI persona generation and customization; (ii) age verification and eligibility compliance; and (iii) fraud detection and platform security. Facial recognition data shall be deleted immediately upon completion of persona generation and shall not be retained for any supplementary purpose except as legally mandated.

(e) Geolocation and Approximate Location Data

The Company infers approximate geographic location from:

- Internet Protocol (IP) address geolocation databases
- Global Positioning System (GPS) data (only if User has explicitly enabled location services)
- Cell tower triangulation information (only if transmitted by User device)
- WiFi network geographic correlation

Important Limitation: The Company does not request, collect, or store precise real-time location data.

(f) Third-Party Platform Linkage Data

If User authenticates through federated identity providers (Facebook, Google, Apple, Discord), the Company receives:

- Email addresses verified by third-party identity providers
- User profile names and identifiers
- Avatar images and profile photographs
- Limited public profile information (subject to OAuth 2.0 scope restrictions)

1.3 Information Derived from Third Parties

(a) Complementary Data Sources

The Company may augment User profiles with information derived from:

- Credit reporting agencies and consumer credit bureaus (limited to verification purposes)
- Age verification and identity confirmation services
- Fraud detection services and behavioral analytics platforms
- Public records and municipal databases
- Data aggregators and information brokers
- Other Users' submissions (e.g., when another User uploads contact lists containing User's information)

(b) Contractual Third-Party Recipients

Information may be received from service providers with whom Users have independently contracted, including cloud storage providers, social media platforms, and affiliate services.

2. STATUTORY BASIS FOR INFORMATION PROCESSING

2.1 GDPR Article 6 and Article 9 Lawful Processing Bases

For Users subject to GDPR jurisdiction (European Economic Area, United Kingdom, Switzerland), the Company processes personal data pursuant to the following independent and alternative lawful bases:

(a) Contractual Performance (GDPR Article 6(1)(b))

Processing constitutes a necessary prerequisite to contract formation and performance. User cannot access the Platform without submission of minimal requisite information, thereby establishing a binding contractual nexus.

(b) Legitimate Interests (GDPR Article 6(1)(f))

The Company maintains compelling legitimate interests in:

- Platform security and cybersecurity threat mitigation
- Fraud detection, prevention, and remediation
- Platform abuse and terms-of-service violation identification
- Service quality optimization and technical infrastructure improvement
- Aggregate statistical analysis and business intelligence development
- Risk management and regulatory compliance assurance
- Legal defense preparation and evidentiary preservation

These legitimate interests have been subjected to comprehensive balancing against User privacy interests and fundamental rights and have been determined to outweigh User privacy expectations.
(c) Affirmative Consent (GDPR Article 6(1)(a) and Article 9(2)(a))

User affirmatively consents to:

- Processing of personal data for service provision and optimization
- Retention of user-generated content for AI model refinement and training
- Utilization of behavioral data for personalization and feature recommendation
- Aggregation of anonymized usage metrics for research purposes

Such consent may be withdrawn at any time by User notification to support@imagiportal.me, provided that such withdrawal does not affect the lawfulness of processing predating withdrawal.

(d) Legal Obligation (GDPR Article 6(1)(c))

Processing is mandated to satisfy statutory obligations including:

- Tax authority reporting requirements
- Government agency compliance demands
- Judicial proceedings and law enforcement cooperation
- Financial services anti-money laundering regulations
- Child safety protection mandates

(e) Special Category Personal Data Processing (GDPR Article 9)

Biometric data processing is justified under GDPR Article 9(2)(a) (explicit consent) and Article 9(2)(b) (employment or social security purposes) to the extent applicable. Age verification processing relies on Article 9(2)(a) (explicit consent) and Article 9(2)(h) (safeguarding vital interests and healthcare purposes).

2.2 CCPA Statutory Framework and Permissible Processing

For Users domiciled in California, the Company processes personal information pursuant to California Consumer Privacy Act statutory authority, specifically:

- Collection of information to deliver products and services requested by the consumer
- Service providers operating under restricted data use limitations
- Business purposes as defined in California Civil Code § 1798.140(w)
- Automated decision-making and profiling practices as disclosed in this Policy

3. COMPREHENSIVE METHODOLOGY AND UTILIZATION PURPOSES

3.1 Platform Operations and Service Delivery

(a) Essential Service Functions

User information is processed for:

- Account establishment, authentication, and access credential verification AI persona instantiation and architectural configuration
- Chat interface operation and conversational AI engagement
- Voice processing and acoustic data synthesis
- Image generation and manipulation processing
- Storage allocation and computational resource allocation

(b) Security and Abuse Prevention

User information is processed to:

- Implement multi-factor authentication protocols
- Detect and mitigate unauthorized account access
- Prevent spam, fraudulent transactions, and phishing attacks
- Identify Terms of Service violations and policy breaches
- Prevent dissemination of child sexual abuse material (CSAM)
- Detect and remediate deepfake generation and non-consensual intimate imagery
- Prevent scraping, data harvesting, and automated access
- Implement rate limiting and resource consumption restrictions

(c) Platform Optimization and Continuous Improvement

User information is processed to:

- Analyze aggregate usage patterns and feature adoption rates
- Identify technical bottlenecks and performance degradation
- A/B test interface modifications and feature implementations
- Optimize computational efficiency and infrastructure resource allocation
- Develop successor products and enhanced feature implementations
- Conduct machine learning model refinement and algorithmic optimization

3.2 Personalization and Algorithmic Content Delivery

User information is processed to:

- Generate persona-specific content recommendations
- Curate personalized discovery feeds
- Implement machine learning-driven suggestion algorithms
- Tailor user interface presentation to individual preferences
- Optimize feature prioritization based on individual usage patterns

3.3 Marketing, Promotional, and Commercial Communications

Affirmative Consent-Based Marketing

User information is processed to send promotional materials, product updates, service announcements, and commercial messages exclusively upon User affirmative opt-in. Users may opt out of marketing communications at any time through account settings or by clicking unsubscribe links contained in marketing communications.

3.4 Compliance, Regulatory, and Legal Obligations

User information is processed to:

- Satisfy tax authority reporting requirements
- Comply with governmental investigatory demands and legal process
- Enforce Terms of Service and Policy compliance
- Defend legal proceedings and regulatory investigations
- Preserve evidence in anticipation of litigation
- Satisfy anti-money laundering and know-your-customer requirements
- Comply with child protection and COPPA mandates

3.6 Aggregate Analytics and De-Identified Research

User information may be aggregated, pseudonymized, and de-identified for research, business intelligence, and academic purposes. Such information does not constitute "personal data" and is not subject to this Policy's restrictions.

4. DATA RETENTION, DELETION, AND LIFECYCLE MANAGEMENT

4.1 Retention Schedule by Data Category

(a) Account Information and Registration Data

- Retention Duration: Maintained for duration of account active status, plus thirty six (36) months following account termination or deletion
- Justification: Necessary for dispute resolution, regulatory compliance, and fraud investigation
- Deletion Methodology: Secure deletion using cryptographic overwriting protocols.

(b) User-Generated Content (Personas, Prompts, Conversations)

- Default Retention: Retained during account active status
- Upon Account Deletion: Retained for ninety (90) days in backup systems to permit restoration; permanent deletion thereafter
- Optional Extended Retention: User may elect to retain content indefinitely

(c) Biometric and Facial Recognition Data

- Retention Duration: Deleted immediately upon completion of AI persona generation process
- No Secondary Retention: Under no circumstances shall facial recognition data be stored, retained, or processed for supplementary purposes
- Exception: Age verification biometric data may be retained for thirty (30) days to permit verification challenge and dispute resolution

(d) Usage Analytics and Telemetry Data

- Retention Duration: Twenty-four (24) months from collection timestamp
- Aggregation: Data shall be aggregated and pseudonymized within one hundred eighty (180) days of collection

(e) Payment Transaction History

- Retention Duration: Maintained for seven (7) years as mandated by tax authority requirements and financial services regulations
- PCI DSS Compliance: Limited to merchant category codes, transaction amounts, timestamps, and card last-four digits

(f) Device and Technical Data

- Retention Duration: Twelve (12) months from collection timestamp
- Security Logs: Device-level security and authentication logs retained for thirty (30) months for forensic investigation purposes

(g) Customer Support Communications

- Retention Duration: Maintained for thirty-six (36) months from final communication timestamp
- Justification: Necessary for dispute resolution and service quality assurance

(h) Audit Logs and System Administration Records

- Retention Duration: Seven (7) years from log generation timestamp
- Justification: Necessary for regulatory compliance, forensic investigation, and legal defense

(i) Cookies and Session Data

- Retention Duration: Session-based cookies deleted upon browser termination; persistent cookies retained per cookie-specific retention policies (typically twelve (12) months)

4.2 Deletion Procedures and User Rights

(a) Right to Erasure (GDPR Article 17)

Users may request deletion of personal data subject to the following exceptions:

- Contract Performance Exception: Data necessary for contract performance may not be deleted
- Legal Obligation Exception: Data maintenance as required by applicable law may not be deleted
- Legitimate Interest Exception: Data processing justified by legitimate interests may be maintained if such interests outweigh User erasure rights
- Public Interest Exception: Data processing necessary for public interest purposes may be maintained
- Archival Exception: Data maintained for archival, research, and statistical purposes may be maintained in pseudonymized form

(b) Right to Data Portability (GDPR Article 20)

Users may request export of personal data in machine-readable format (JSON, CSV, XML) within thirty (30) days of request submission. Such data shall include:

- Account information and registration data
- All user-generated content and communications
- Usage analytics and behavioral data (pseudonymized where possible)
- Transaction history and billing records

(c) Right to Rectification (GDPR Article 16)

Users may request correction of inaccurate, incomplete, or outdated personal data. The Company shall update records within thirty (30) days of verified request submission.

(d) Right to Restrict Processing (GDPR Article 18)

Users may request that the Company restrict processing of personal data pending dispute resolution, legal proceedings, or other circumstances. During restriction periods, data shall be maintained but not processed except as necessary for legal defense or regulatory compliance.

4.3 Secure Deletion Protocols

The Company implements the following deletion methodologies to ensure irreversible data destruction:

- Primary Data Deletion: Cryptographic overwriting using pseudorandom data (DOD 5220.22-M or NIST 800-88 guideline compliance minimum)
- Database Deletion: Parameterized queries and row-level deletion with transaction logging and audit trails
- Backup System Deletion: Data retention in backup and disaster recovery systems limited to ninety (90) days following primary deletion
- Third-Party Deletion: Service providers instructed to implement equivalent deletion protocols within contracted data processing agreements
- Verification: Cryptographic hash verification confirming successful deletion

5. INTERNATIONAL DATA TRANSFER AND CROSS BORDER PROCESSING

5.1 Data Transfer Mechanisms

User data may be transferred to and processed in jurisdictions outside User's residence, including the United States, European Union member states, and other countries where the Company maintains infrastructure or engages service providers. The Company implements the following safeguards:

(a) Standard Contractual Clauses (SCC)

For transfers from the European Economic Area to non-adequate jurisdictions, the Company executes Standard Contractual Clauses as approved by the European Commission and incorporated into Data Processing Agreements with all recipients.

(b) Binding Corporate Rules (BCR)

The Company operates under corporate-wide binding data protection rules applicable to all affiliated entities, subsidiaries, and contractors, ensuring consistent protection across jurisdictional boundaries.

(c) Adequacy Decisions

For transfers to jurisdictions with European Commission adequacy determinations (Canada, Israel, Japan, New Zealand, Switzerland), data transfers proceed without supplementary safeguards.

(d) Supplementary Technical and Organizational Measures

For transfers to jurisdictions without adequacy determinations, the Company implements supplementary protective measures including:

- End-to-end encryption preventing third-party disclosure

- Pseudonymization and data aggregation
- Purpose limitation and access restriction protocols
- Regular security audits and compliance certifications

5.2 Data Subject Rights Across Jurisdictions

Regardless of data storage location, Users retain statutory rights under their jurisdiction of residence or citizenship, including GDPR rights for EU residents, CCPA rights for California residents, and equivalent rights under other applicable statutory regimes.

6. THIRD-PARTY RECIPIENTS AND DISCLOSURE LIMITATIONS

6.1 Service Providers and Data Processors

The Company engages the following categories of service providers to provide essential platform functions, subject to Data Processing Agreements incorporating Standard Contractual Clauses and equivalent protective provisions:

(a) Infrastructure and Hosting Services

- Amazon Web Services (AWS)
- Google Cloud Platform
- Microsoft Azure
- Lambda Labs
- Cloudflare content delivery networks

(b) Payment Processing and Financial Services

- Stripe
- PayPal
- Cryptocurrency payment processors

(c) Analytics and Business Intelligence

- Google Analytics

(d) Customer Support and Communication

N/A

(e) Security and Fraud Prevention

N/A

(f) Marketing and Advertising

- Google Ads
- Facebook Pixel
- Reddit Ads
- X Ads

Programmatic advertising networks

Contractual Safeguards: All service providers are contractually obligated to process personal data only as directed by the Company, maintain adequate security measures, subcontract only upon Company approval, and provide equivalent statutory protections to Users.

6.2 Legal Process and Governmental Disclosure

The Company may disclose personal data in response to:

- Subpoenas, court orders, and judicial process
- Administrative summonses and governmental investigatory demands
- National security letters (NSLs) and Foreign Intelligence Surveillance Act (FISA) requests
- Law enforcement requests under 18 U.S.C. § 2702 and equivalent state statutory frameworks
- Child protection and COPPA compliance demands

Transparency Commitment: Except when legally prohibited from disclosure, the Company shall:

- Notify affected Users of governmental data requests within thirty (30) days Assert legally cognizable objections to overbroad or unreasonable requests
- Disclose only personal data expressly identified in legal process
- Preserve Users' opportunity to seek judicial modification of disclosure orders

6.3 Business Transfers and Insolvency Proceedings

In the event of merger, acquisition, bankruptcy, or asset sale, User personal data may be transferred to successor entities, subject to:

- Notice to affected Users prior to transfer or within thirty (30) days of transfer completion
- User opportunity to object to transfer or request deletion
- Binding obligations on successors to maintain substantially equivalent privacy protections
- Successor entity adoption of this Policy or provision of equivalent protections

6.4 Limitations on Consent-Based Disclosure

Absent affirmative User authorization, the Company shall not disclose personal data to unaffiliated third parties except as expressly provided in this Policy.

7. INFORMATION SECURITY AND PROTECTIVE MEASURES

7.1 Technical Security Architecture

The Company implements a comprehensive information security program encompassing:

(a) Encryption and Data Confidentiality

- Data in Transit: Transport Layer Security (TLS) 1.3 minimum encryption for all data transmission; HTTPS protocol enforcement; certificate pinning for critical connections
- Data at Rest: Advanced Encryption Standard (AES-256) encryption for all databases and file storage systems; encrypted key management services (AWS KMS, Google Cloud KMS)
- End-to-End Encryption: Optional E2EE for sensitive communications within persona-to-user and user-to-user communications
- Cryptographic Key Management: Hardware security module (HSM) storage of encryption keys; automatic key rotation every ninety (90) days; segregation of keys from encrypted data

(b) Access Control and Authentication

- Multi-Factor Authentication (MFA): Mandatory MFA for administrative accounts; optional MFA for User accounts
- Role-Based Access Control (RBAC): Principle of least privilege implemented across all systems; administrative access limited to minimum necessary personnel
- Single Sign-On (SSO): OAuth 2.0 and Security Assertion Markup Language (SAML) integration for enterprise federated authentication
- Session Management: Cryptographically random session tokens; automatic session expiration after fifteen (15) minutes of inactivity
- Privileged Access Management (PAM): Vault-based credential management; just in-time administrative access provisioning

(c) Network Security and Perimeter Defense

- Web Application Firewall (WAF): Cloudflare/AWS WAF implementation blocking common attack vectors (SQL injection, cross-site scripting, cross-site request forgery)
- Distributed Denial-of-Service (DDoS) Protection: BGP-based DDoS mitigation; rate limiting; IP reputation filtering
- Network Segmentation: Virtual Private Cloud (VPC) architecture; separate network zones for databases, application servers, and administrative systems
- Intrusion Detection and Prevention: Snort/Suricata-based network intrusion detection systems; anomaly detection algorithms
- Vulnerability Scanning: Automated network vulnerability scanning; monthly penetration testing; annual red team exercises

(d) Application Security and Code Quality

- Secure Software Development Lifecycle (SSDLC): Threat modeling; secure design review; code review processes; static application security testing (SAST)
- Dependency Management: Software composition analysis; vulnerability scanning of third-party

libraries; automated dependency updates
- Container Security: Image scanning for vulnerable packages; registry authentication; container runtime security monitoring
- API Security: OAuth 2.0 and OpenID Connect implementation; API key rotation; rate limiting and throttling

7.2 Organizational Security Controls

(a) Personnel Security

- Background Investigations: Comprehensive background checks for all personnel with data access
- Confidentiality Agreements: Non-disclosure agreements and restrictive covenants executed by all employees and contractors
- Security Training: Annual mandatory security awareness training; role-specific security training; phishing simulation exercises
- Segregation of Duties: Incompatible duty assignments segregated to prevent fraud and unauthorized access
- Termination Procedures: Immediate credential revocation, system access removal, and badge deactivation upon employment termination

(b) Audit and Compliance

- Logging and Monitoring: Centralized logging (ELK Stack, Splunk) of all access events; twelve (12) month retention; real-time alerting for anomalous activity
- SOC 2 Type II Compliance: Annual third-party audits of security and operational controls; remediation of audit findings
- ISO 27001 Certification: Annual certification and recertification against ISO/IEC 27001:2022 information security standards
- Incident Response Planning: Formal incident response procedures; 24/7 security operations center (SOC) monitoring; incident classification and escalation protocols
- Disaster Recovery and Business Continuity: Recovery Time Objective (RTO) of four (4) hours; Recovery Point Objective (RPO) of one (1) hour; annual disaster recovery testing

7.3 Limitations on Security

NOTWITHSTANDING THE COMPREHENSIVE SECURITY MEASURES DELINEATED ABOVE, THE COMPANY PROVIDES NO ABSOLUTE GUARANTEE OR UNQUALIFIED REPRESENTATION THAT PERSONAL DATA SHALL REMAIN FREE FROM UNAUTHORIZED DISCLOSURE. NO METHOD OF TRANSMISSION ACROSS THE INTERNET AND NO METHOD OF ELECTRONIC STORAGE IS COMPLETELY IMPERVIOUS TO COMPROMISE, INTERCEPTION, OR UNAUTHORIZED ACCESS. USER ACKNOWLEDGES INHERENT RISKS ASSOCIATED WITH INTERNET TRANSMISSION AND ACCEPTS SUCH RISKS. THE COMPANY DISCLAIMS LIABILITY FOR UNAUTHORIZED ACCESS, DISCLOSURE, MODIFICATION, OR DESTRUCTION OF PERSONAL DATA RESULTING FROM EVENTS BEYOND ITS REASONABLE CONTROL, INCLUDING ZERO-DAY VULNERABILITIES, ADVANCED PERSISTENT THREATS (APT), STATE SPONSORED ATTACKS, AND FORCE MAJEURE EVENTS.

8. CHILDREN'S PRIVACY AND COPPA COMPLIANCE

8.1 Age Eligibility Requirements

The Platform is strictly limited to individuals eighteen (18) years of age or older. THE COMPANY DOES NOT KNOWINGLY, INTENTIONALLY, OR WITH RECKLESS DISREGARD COLLECT, SOLICIT, OR PROCESS PERSONAL INFORMATION FROM MINORS UNDER THIRTEEN (13) YEARS OF AGE IN VIOLATION OF THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT, 15 U.S.C. § 6501 et seq.

8.2 Verification and Age Gating

The Company may implement age verification mechanisms which may include:

- Affirmative representation that User is eighteen (18) or older at registration
- Age verification through third-party services
- Government-issued photographic identification submission and verification
- AI-based facial age estimation (non-storing of facial data for verification purposes)
- Credit card verification (inherently restricts to individuals with established credit history)

8.3 Parental Notification and Deletion

If the Company discovers that personal information from a child under thirteen (13) years of age has been collected or processed, the Company shall:

- Immediately cease processing of such information
- Provide notice to the child's parent or legal guardian
- Delete all collected personal information within ten (10) business days
- Cooperate with parent/guardian requests for verification of deletion

Parents or legal guardians who believe the Company has collected information from a child under thirteen (13) should contact coppa@imagiportal.me with supporting documentation of the child's age.

9. CALIFORNIA PRIVACY RIGHTS (CCPA) AND SIMILAR STATE REGIMES

9.1 Right to Know (CCPA § 1798.100)

California residents possess the statutory right to request disclosure of:

- Specific personal information collected and processed
- Purposes for collection and processing
- Categories of sources from which information was collected

- Categories of third parties with whom information was shared
- Business purposes for collection and retention

Such requests shall be honored within forty-five (45) days and shall be provided without cost.

9.2 Right to Delete (CCPA § 1798.105)

California residents possess the statutory right to request deletion of personal information collected and processed, subject to statutory exceptions including:

- Completion of requested transactions
- Security operations and fraud prevention
- Compliance with legal obligations
- Internal uses reasonably aligned with User expectations
- Improvement of Platform functionality
- Compliance with California Consumer Privacy Act

9.3 Right to Opt-Out of Sale or Sharing (CCPA § 1798.120)

California residents possess the right to direct the Company to cease "sale" or "sharing" of personal information as those terms are defined in California law. THE COMPANY DOES NOT KNOWINGLY "SELL" PERSONAL INFORMATION AS DEFINED IN CCPA § 1798.140(ag). THE COMPANY MAY "SHARE" PERSONAL INFORMATION WITH THIRD-PARTY ADVERTISING PARTNERS FOR CROSS-CONTEXT BEHAVIORAL ADVERTISING. CALIFORNIA RESIDENTS MAY OPT OUT OF SUCH SHARING THROUGH:

- Account settings and privacy preferences
- "Do Not Sell or Share My Personal Information" link on Platform homepage
- California Privacy Rights Foundation opt-out list

9.4 Nondiscrimination Prohibition (CCPA § 1798.125)

The Company shall not discriminate against California residents who exercise their statutory rights, including by:

- Denying services or features
- Charging differential prices or fees
- Providing inferior quality or service
- Suggesting differential treatment

Exception: The Company may offer financial incentives for data collection that are reasonably related to collection value and proportionate to such value.

9.5 Virginia, Colorado, Connecticut, Utah, and Additional State Privacy Statutes

The Company extends substantially equivalent privacy rights to residents of states with comprehensive privacy statutes (Virginia Consumer Data Protection Act, Colorado Privacy Act, Connecticut Data Privacy Act, Utah Consumer Privacy Act, Delaware Personal Privacy Act) and similar state-level privacy frameworks.

10. EXTERNAL LINKS AND THIRD-PARTY SERVICES

The Platform may contain hyperlinks to third-party websites, applications, and services not operated or controlled by the Company, including social media platforms, analytics providers, and content delivery networks. The Company disclaims responsibility for the privacy practices, terms of service, security measures, content, or operational policies of such third-party services. Users are advised to review applicable privacy policies and terms of service prior to engaging with third-party services. The Company shall not be held liable for any harm, loss, or damage resulting from User engagement with third-party services or reliance upon third-party privacy representations.

11. CHANGES TO PRIVACY POLICY

11.1 Amendment Procedures

The Company may modify, supplement, amend, or replace this Privacy Policy at any time and at its sole discretion. Material modifications shall be communicated via:

- Prominent notice on the Platform homepage
- Electronic mail notification to registered User email addresses
- In-app notifications and alerts
- Posting of updated Policy with revised effective date

11.2 Effective Date and Retroactivity

Updated Policies become effective upon posting. User continued utilization of the Platform following Policy modification constitutes acknowledgment and acceptance of revised terms. Users who do not accept modified terms must discontinue Platform access.

11.3 Preservation of Historical Policy Versions

Previous versions of this Privacy Policy shall be archived and maintained at imagiportal.me/privacy-policy-archive for historical reference.

12. EUROPEAN DATA PROTECTION RIGHTS AND GDPR SPECIFIC PROVISIONS

12.1 Data Protection Officer (DPO) Contact

Users subject to GDPR jurisdiction may contact the Company's Data Protection Officer at dpo@imagiportal.me regarding data protection matters, privacy concerns, and potential violations.

12.2 Supervisory Authority Contact

Users who believe their data protection rights have been violated may file a complaint with their competent data protection authority:

- European Data Protection Board (EDPB)
- National data protection authorities within their member state
- Information Commissioner's Office (ICO) for United Kingdom residents

12.3 Data Protection Impact Assessment (DPIA)

The Company conducts comprehensive Data Protection Impact Assessments prior to implementing new processing activities, particularly those involving:

- Large-scale systematic processing of special category data
- Automated decision-making with legal or similarly significant effects
- Systematic monitoring of public areas

DPIAs shall be made available to supervisory authorities upon request.

12.4 Data Processing Agreement (DPA)

For Users or organizations qualifying as data controllers or utilizing the Platform for commercial processing, the Company provides a Data Processing Agreement incorporating:

- Standard Contractual Clauses
- Appropriate safeguards and supplementary measures
- Sub-processor authorization and notification procedures
- Audit and inspection rights

13. DISPUTE RESOLUTION AND REGULATORY COMPLAINTS

Users with privacy concerns or disputes may pursue resolution through:

- Informal Resolution: support@imagiportal.me
- Data Protection Officer Review: dpo@imagiportal.me
- Supervisory Authority Complaint: National data protection authority
- Binding Arbitration: As provided in the Terms of Service

14. CONTACT INFORMATION AND REQUESTS

Privacy Inquiries and Data Subject Rights Requests:
Email: support@imagiportal.me

Mailing Address:
ImagiPortal Inc.
Privacy Team
1111B S Governors Ave STE 26293
Dover, DE 19904
United States

Data Protection Officer:
Email: dpo@imagiportal.me

COPPA/Children's Privacy Issues:
Email: coppa@imagiportal.me

Requests must include:

- User identification and account information
- Specific nature of request (data access, deletion, portability, rectification, etc.)
- Supporting documentation of identity verification
- Preferred communication method and language

All requests shall be processed within forty-five (45) days or within statutory timeframe if more stringent.

15. FINAL PROVISIONS

15.1 Severability

If any provision of this Privacy Policy is determined to be invalid, illegal, or unenforceable by a court of competent jurisdiction, such provision shall be severed, and remaining provisions shall continue in full force and effect. The parties agree to negotiate in good faith to replace any severed provision with valid language achieving the original intent.

15.2 Entire Agreement

This Privacy Policy, in conjunction with the Terms of Service, constitutes the complete and exclusive agreement regarding privacy, data protection, and personal information handling. All prior negotiations, understandings, and agreements are superseded.

15.3 Governing Law

Governing Law and Dispute Resolution This Privacy Policy shall be governed by and construed in accordance with the substantive laws of the State of Delaware, without regard to its conflict of law principles. Any dispute, controversy, or claim arising out of or relating to this Privacy Policy, including the validity, invalidity, breach, or termination thereof, shall be resolved exclusively according to the Dispute Resolution, Binding Arbitration, and Class Action Waiver procedures set forth in Section 12 of the Terms of Service. You explicitly agree that the exclusive venue and jurisdiction for any such disputes shall be as defined in the Terms of Service.

15.4 Waiver

No waiver of any provision of this Privacy Policy shall constitute a waiver of any other provision, nor shall any waiver constitute a continuing waiver absent written acknowledgment.

PRIVACY POLICY ACKNOWLEDGMENT

By accessing or utilizing ImagiPortal, User irrevocably acknowledges having read, understood, and agreed to be bound by this Privacy Policy in its entirety. User further acknowledges understanding that this Policy, in conjunction with the Terms of Service, comprises binding legal instruments establishing comprehensive rights and obligations regarding personal data collection, processing, utilization, and retention.

Date Last Updated: January 17, 2026
Effective Date: January 17, 2026
Version: 2.0