

Moonlit One Enterprise Privacy Policy & Data Processing Terms

1/4

This Privacy Policy and Data Processing Agreement governs the data collection, security obligations, and liability frameworks for Moonlit One, an Identity-as-a-Service (IDaaS) and single sign-on (SSO) infrastructure platform provided by The Moonlit Company. Moonlit One is designed to centralize and secure application access for enterprise business operations.

1. Data Controller and Data Processor Roles

Moonlit One operates strictly as a B2B enterprise platform. We do not offer services directly to individual consumers.

Data Controller: The enterprise customer utilizing Moonlit One retains full ownership, control, and legal responsibility for all employee and organizational data routed through the platform.

Data Processor: The Moonlit Company acts solely as a data processor, handling data explicitly on the documented instructions of the enterprise customer to facilitate secure authentication.

No Monetization: We do not sell, rent, or utilize customer data for marketing, profiling, or training external machine learning models.

2. Information Collection and Scope

Our data collection is strictly limited to the necessary components required to securely authenticate cross-application sessions.

Identity and Credential Data: We collect corporate email addresses, designated user roles, organizational identifiers, and the cryptographic identity tokens required for SSO handoffs.

Telemetry and Security Logs: We automatically log session metadata, IP addresses, device identifiers, authentication timestamps, and network traffic for security auditing and anomaly detection.

Customer Configurations: We store organizational directories and application integration settings as configured by the enterprise administrator.

Moonlit One Enterprise Privacy Policy & Data Processing Terms

2/4

3. Permitted Utilization of Data

Data routed through Moonlit One is utilized exclusively for platform functionality and security.

Authentication Routing: Tokens and credentials are used to verify user permissions and grant secure access to connected internal and third-party enterprise applications.

Security Auditing: Access logs are continuously monitored to detect unauthorized access attempts, mitigate DDoS attacks, and enforce compliance with internal security mandates.

Service Optimization: We process system data to maintain high availability, route global traffic efficiently, and resolve technical support escalations.

4. Limitation of Liability and Risk Allocation

The Moonlit Company provides the authentication infrastructure but explicitly disclaims liability for the underlying applications or customer misconfigurations.

Exclusion of Consequential Damages: Under no circumstances shall The Moonlit Company be liable for indirect, incidental, special, punitive, or consequential damages. This includes, but is not limited to, lost profits, lost revenue, business interruption, or reputational harm, regardless of prior disclosure of such potential damages.

General Liability Cap: The aggregate cumulative liability of The Moonlit Company for any claims arising from or related to the use of Moonlit One is strictly capped at the total subscription fees paid by the enterprise customer in the twelve (12) months immediately preceding the event giving rise to the claim.

Customer Indemnification: The enterprise customer agrees to fully indemnify and hold The Moonlit Company harmless against any third-party claims, regulatory fines, or damages resulting from the customer's violation of data privacy laws or the transmission of unauthorized sensitive data through the Moonlit One infrastructure.

Moonlit One Enterprise Privacy Policy & Data Processing Terms

3/4

5. Security Standards and Incident Response

We implement comprehensive security architectures to protect enterprise data in transit and at rest.

Encryption Standards: All data in transit is secured via TLS 1.3. Identity tokens and stored credentials are encrypted at rest utilizing AES-256 encryption.

Infrastructure Security: We maintain alignment with SOC 2 Type II and ISO 27001 frameworks. Enterprise customers are granted standard audit rights limited to reviewing third-party attestation reports to ensure multi-tenant infrastructure security.

Breach Notification: In the event of a verified security incident affecting customer data, we will notify the designated enterprise security contact within 72 hours and provide necessary telemetry for the customer to fulfill regulatory obligations.

6. Sub-Processors and Third-Party Integrations

To deliver high-availability service, we engage vetted infrastructure partners.

Authorized Sub-Processors: We utilize tier-one cloud hosting and network sub-processors. Customers will receive advance notice of any new sub-processor additions and maintain the right to object based on documented security concerns.

Third-Party Application Disclaimers: Moonlit One acts as the gateway to third-party applications chosen by the customer. We accept no liability for the data practices, security postures, or uptime of these third-party platforms once the authentication handoff is complete.

7. Data Retention and Post-Termination

Enterprise data lifecycle management is automated to ensure compliance with data minimization principles.

Moonlit One Enterprise Privacy Policy & Data Processing Terms

4/4

Session Purging: Authentication tokens and temporary session identifiers are purged immediately upon session expiration or manual termination.

Log Retention: Security access logs are retained for a standard 12-month trailing period for compliance and audit purposes before permanent deletion.

Post-Termination Deletion: Upon termination of the enterprise service agreement, all associated customer routing configurations and identity metadata are permanently deleted from our active servers within 60 days.

8. Policy Management

All legal documentation governing Moonlit One, including comprehensive terms, sub-processor agreements, and historical policy versions, is centrally managed. For full documentation and policy updates, please visit moonlit.company/legal.