

Oneasy SaaS Privacy Policy

Last Updated Date: June 25, 2026

Effective Date: June 25, 2026

GloryScience International Limited, a company incorporated under the laws of the Hong Kong Special Administrative Region ("**GloryScience**", "**we**", "**us**", or the "**Company**"), is the operator of the Oneasy SaaS Platform ("**Oneasy**" or the "**Service**"). We recognize the importance of personal information and are committed to providing reasonable, appropriate protection that is proportionate to the nature of the Service. This SaaS Service Privacy Policy (this "**Policy**") is intended to explain, in a clear and transparent manner, how GloryScience processes your personal information when you use the Oneasy website, the Oneasy SaaS platform, or otherwise interact with us.

This Policy forms part of the Oneasy SaaS Service Agreement (the "**Main Agreement**"). With respect to personal data processing matters, if this Policy conflicts with the data processing agreement signed by the parties or incorporated by reference (where applicable), or with mandatory requirements of applicable law, the applicable data processing agreement or mandatory legal requirements shall prevail. With respect to specific security controls, remote access security, incident response, log retention, and technical and organizational measures, the applicable Security Addendum, DPA, or other security document separately agreed by the parties shall prevail. Your specific rights and obligations are ultimately determined by the applicable data protection laws that have jurisdiction over you or the relevant processing activities, as well as any jurisdiction-specific supplemental terms that we may publish. Please read this Policy carefully before using our Service. If you do not agree with any part of this Policy, please do not use our Service.

I. Scope and Role Definitions

1.1 Scope of this Policy

This Policy applies to your use of or access to the following services provided by us: the Oneasy website, including www.oneasy.cc and its subdomains; the Oneasy SaaS platform; and the related APIs, support channels, and sales communications.

This Policy does not apply to any website, application, or service operated by a third party, even if you access it through our Service.

1.2 Key Role Definitions

Under major global data protection laws, we may act in different legal roles in different data processing scenarios:

(A) GloryScience as a "Controller"

For personal information that is necessary to provide, operate, protect, and improve our Service, we may act as a controller. This typically includes your account information; billing and transaction information; service usage logs and diagnostic data; security and compliance logs; and information collected through cookies and similar technologies for website operation, analytics, security protection, and service optimization.

(B) GloryScience as a "Processor"

For any data that you, as our "Tenant", upload, generate, or manage when using the Oneasy Service ("**Tenant Data**"), GloryScience generally acts as a processor. Tenant Data may include device information, network configurations, performance metrics, and operational logs managed by you. In this role, GloryScience processes

Tenant Data only in accordance with the Main Agreement, the DPA, and your configuration instructions within the Service. For personal data contained in Tenant Data, GloryScience's specific obligations as a processor shall be governed by the applicable DPA.

(C) Tenant as "Controller"

As the Tenant, you are the controller or equivalent responsible party for your Tenant Data, and you independently bear responsibility for complying with all privacy, data protection, communications confidentiality, telecommunications regulatory, cybersecurity, and other laws applicable to your data processing activities, including ensuring that you have a lawful basis for processing such data.

1.3 Interpretation of Roles in Non-GDPR Jurisdictions

Where applicable law does not use the terms "Controller" or "Processor", or where those terms have different meanings, the references in this Policy to controller, processor, tenant, and service provider shall be interpreted by reference to the functionally closest roles and obligations under such law. Such interpretation shall not expand GloryScience's statutory obligations beyond the scope expressly required by applicable law.

II. Information We Collect

We follow the principle of data minimization and collect only the information necessary for specific, explicit, and lawful purposes.

2.1 Account and Configuration Information

To create and manage your account, we collect your name, email address, password, and the position, department, company information, account roles, permission configurations, and other information that you choose to provide.

2.2 Subscription and Payment Information

To process subscriptions and payments, we collect company name, billing address, tax identification number, order records, subscription plan, payment status, and invoice-related information. Payment details, such as complete credit card information, are processed directly by our designated third-party payment service provider that complies with applicable industry standards. We do not store complete payment card information.

2.3 Service Usage and Operational Data

To ensure proper operation of the Service, troubleshoot issues, and improve performance, we automatically collect IP address, device identifiers, browser type, access timestamps, feature usage logs, performance metrics, error reports, login records, API call records, security event records, and other necessary platform operational data.

2.4 Tenant Data

All types of business data that you enter, upload, configure, authorize us to read, permit to be generated, or that are generated by the Service based on your devices, networks, or configurations are Tenant Data. The specific content of Tenant Data is controlled by you, and we, as processor, are not responsible for such content. The Tenant shall independently confirm whether the data it uploads, accesses, transmits, processes, or authorizes GloryScience to process through the Oneasy Service is subject to applicable telecommunications regulatory laws, communications confidentiality laws, cybersecurity laws, or data protection laws.

Tenant Data may include ISP network device configuration information, IP addresses, MAC addresses, device identifiers, OLT / ONU information, network topology, operation and maintenance logs, fault and alarm records, performance metrics, telemetry data, remote access logs, SNMP walk results, CLI/API outputs, configuration backups, packet capture files, diagnostic results, or analysis results. In certain jurisdictions, such data may be

regarded as personal data, regulated telecommunications data, communications metadata, cybersecurity data, commercially sensitive information, or data related to critical infrastructure. The Tenant shall make its own assessment and bear the corresponding compliance responsibilities.

The Customer's acceptance of the Main Agreement, creation of a tenant, addition of devices, configuration of credentials, enablement of Agent / VPN / Connector / API / SNMP / TR-069 / TR-369 / CLI / Syslog / ACS / NMS interfaces, upload or submission of MIBs, OIDs, SNMP walk results, CLI/API outputs, configuration backups, logs, packet capture files, scripts, templates, device materials, vendor materials, or other third-party technical materials, or authorization for Oneasy to read, generate, or process such materials, constitutes the Customer's instruction and authorization for GloryScience to process the relevant Tenant Data for personal data protection purposes.

For the avoidance of doubt, this Policy primarily describes the processing of personal information and the portion of Tenant Data that constitutes personal data. For MIBs, OIDs, SNMP walks, CLI/API outputs, OMCI materials, firmware materials, device vendor materials, vendor internal documents, configuration templates, scripts, packet capture files, log samples, or other third-party technical materials that the Customer provides, uploads, submits, configures, references, authorizes to be read, or permits to be generated through the Oneasy Service, except for the portions that contain personal data, the source of rights, usage authorization, confidentiality obligations, intellectual property rights, trade secret restrictions, and allocation of responsibility shall be governed by the Main Agreement, Security Addendum, Order Form, SOW, or special terms for technical materials.

2.5 Communications Records

When you contact our support team, participate in sales consultations, submit tickets, attend training, or provide feedback, we may retain the relevant communications, attachments, and diagnostic information that you voluntarily provide.

2.6 Sensitive Personal Information

If you believe that your use case unavoidably involves sensitive personal information, special categories of personal data, communications content, or other highly sensitive data, you must obtain GloryScience's express written consent before submitting such data, and confirm that you have all necessary lawful bases, notices, consents, authorizations, filings, or approvals. GloryScience may refuse to process such data for reasons relating to security, compliance, technical feasibility, or commercial risk.

2.7 Cookies and Similar Technologies

We may use cookies, log identifiers, and similar technologies to enable website operation, maintain login status, provide security protection, preserve necessary preferences, support payment processes, prevent fraud, or comply with legal requirements. According to the current Cookie Policy, as of the last updated date of that policy, Oneasy does not currently enable non-essential analytics cookies, advertising cookies, marketing cookies, remarketing cookies, cross-site tracking cookies, conversion tracking cookies, or non-essential online chat / customer interaction cookies. For information about cookie types, purposes, retention periods, and management methods, please refer to our Cookie Policy.

2.8 Cloudflare Turnstile Human Verification Service

To prevent automated abuse, malicious registrations, abnormal access, and other security risks, our website may use Cloudflare Turnstile, a human verification service provided by Cloudflare.

When you access or use pages where Turnstile is enabled, your browser may communicate with Cloudflare's servers to complete security verification and determine whether the access request is from a genuine user. Cloudflare may process relevant technical information as necessary for the operation of its service, such as IP address, browser and device-related information, access environment information, and information used for security risk analysis.

This service is used solely for website security protection, reduction of bot attack risks, and maintenance of service reliability. It is not used for advertising or cross-site tracking.

For more information on how Cloudflare collects, uses, and protects relevant information, please refer to the Cloudflare Turnstile Privacy Policy:

<https://www.cloudflare.com/turnstile-privacy-policy/>

III. How We Use Your Information and Legal Bases

We process your personal information only where we have a valid legal basis.

3.1 Performance of Contract

Processing your account information, payment information, and providing core SaaS functionality is necessary for the performance of the Main Agreement entered into with you.

3.2 Legitimate Interests

We process certain information based on our legitimate interests, such as monitoring service security, preventing fraud and abuse, improving services and conducting product development, maintaining platform stability, handling customer support requests, and conducting necessary internal administration. To the extent required by applicable law, we will assess the impact of such processing activities on your privacy and take reasonable measures to reduce unnecessary privacy risks.

Where required by applicable law and reasonably practicable, we may provide descriptions of the relevant processing activities.

3.3 Compliance with Legal Obligations

To comply with tax, accounting, law enforcement, regulatory, security, dispute resolution, or other legal and regulatory requirements, we may process and retain your information where necessary.

3.4 Consent

For processing activities that are not necessary for operation of the Service, such as certain marketing communications, we will obtain your consent where required by applicable law. You have the right to withdraw your consent at any time in accordance with applicable law.

IV. Processing of Tenant Data

4.1 Processing Principles

We process Tenant Data only in accordance with the Main Agreement, applicable DPA, Security Addendum, Order Form, SOW, product functionality, and your configurations, uploads, authorized reads, permitted generation, or other documented instructions within the Service. Your actions, including adding devices, configuring credentials, enabling Agent / VPN / Connector / API / SNMP / TR-069 / TR-369 / CLI / Syslog / ACS / NMS interfaces, uploading or submitting files, authorizing the reading of device outputs, or permitting the generation of SNMP walk results, CLI/API outputs, configuration backups, packet captures, logs, or diagnostic results, may constitute your in-service instructions for processing the relevant Tenant Data.

If we receive an instruction that manifestly violates applicable data protection laws, we reserve the right to refuse to execute such instruction. If we believe that an instruction may violate applicable law, we will, to the extent reasonably practicable, notify you and explain the reason, and provide you with a reasonable opportunity to provide a legal basis or an alternative solution. The parties shall consult in good faith to seek an alternative solution that complies with legal, contractual, and service security requirements. If consultation fails and we reasonably believe that executing the instruction would cause us to incur legal liability, security risks, or violate third-party obligations, we may suspend execution of the relevant instruction, and such suspension shall not constitute a breach of contract.

4.2 Tenant Responsibilities

You represent and warrant that you have the lawful rights and bases to process all Tenant Data; that you have provided all legally required privacy notices to data subjects, subscribers, end users, employees, or other relevant persons; that you have obtained all necessary consents, authorizations, permits, filings, internal approvals, or other lawful bases; and that you have implemented appropriate internal permission management, network isolation, and security controls.

For devices, networks, interfaces, accounts, credentials, MIBs, OIDs, SNMP walk results, CLI/API outputs, OMCI materials, firmware materials, configurations, logs, packet captures, scripts, templates, or other third-party technical materials that are accessed, configured, authorized to be read, permitted to be generated, or processed through the Oneasy Service, you shall independently confirm and obtain all necessary ownership, operation rights, management rights, authorized maintenance rights, disclosure rights, reproduction rights, usage rights, sublicensing rights, confidentiality waivers, device vendor permits, contractual authorizations, regulatory permissions, and end-user notices or consents. We may reasonably rely on your in-service configurations, uploads, submissions, authorized reads, permitted generation, and operation records without separately verifying your authorization chain before each processing activity.

4.3 Assistance Obligations

If a data subject directly exercises rights against us in relation to Tenant Data, such as access, correction, deletion, or restriction of processing requests, we will generally direct that person to contact you as the controller or responsible party for the relevant data. Within reasonable limits, we will assist you in fulfilling your applicable statutory obligations to data subjects through product features, APIs, export functions, or technical support.

V. International Data Transfers

Our Service is global in nature. This means that your personal information may be accessed, processed, or transferred outside the country or region in which you are located.

5.1 Our Safeguards

When personal information is transferred from your jurisdiction to another region, and applicable data protection laws require safeguards for cross-border transfers, we will use legally recognized data transfer mechanisms, such as the EU Standard Contractual Clauses (SCCs), the applicable UK international data transfer mechanisms, or other applicable mechanisms, together with reasonable technical and organizational measures, such as access controls, encryption, logs, and security monitoring, to provide protection.

5.2 Cross-border Processing of Tenant Data

By default, the primary storage region for Tenant Data is the Alibaba Cloud International Singapore region. To provide the Service, improve access performance, support disaster recovery, provide security protection, technical support, Sub-processor services, AI-assisted functions, regional secondary node access, or comply with legal obligations, relevant data may be accessed, processed, cached, backed up, or transferred in other jurisdictions.

We may use Alibaba Cloud International and other evaluated cloud infrastructure, network, CDN, security, logging, monitoring, payment, customer support, and AI service providers as service providers or Sub-processors. The list of material Sub-processors, including their service categories, processing purposes, and primary processing locations, will be published or made available through the Oneasy official website, administrative console, documentation pages, or other reasonable means.

The specific data regions, secondary nodes, disaster recovery nodes, edge nodes, log nodes, cache nodes, backup nodes, support access locations, Sub-processor processing locations, and AI service invocation locations shall be determined by the applicable Main Agreement, DPA, Security Addendum, Order Form, service configuration, Sub-processor list, or written agreement between the parties. Unless expressly agreed otherwise in writing, the description of the primary storage region in this Policy does not constitute a data localization commitment and does not guarantee that all access, processing, caching, backup, logging, technical support, or Sub-processor services will occur only within a single jurisdiction.

The Customer is responsible for completing any cross-border transfer impact assessments, adequacy assessments, notices, consents, filings, or other compliance procedures required in its capacity as controller or equivalent responsible party. This section does not affect our necessary cross-border processing of account, log, payment, support, compliance, and platform operation data as controller for the purposes described in Section III.

VI. Information Sharing and Disclosure

We do not sell your personal information. We share information only in the following circumstances:

- **Service Providers / Sub-processors:** We may share necessary information with partners that provide us with cloud hosting, network, CDN, payment, analytics, communications, security, logging, monitoring, customer support, AI services, or other necessary services ("**Sub-processors**" or "**Service Providers**"). Such partners may include Alibaba Cloud International and other evaluated cloud infrastructure, network, security, logging, monitoring, payment, customer support, and AI service providers. We will take commercially reasonable measures to require relevant service providers to assume confidentiality, data protection, and security obligations appropriate to the nature of their services. For material Sub-processors involved in the processing of Tenant Data, the notification, objection, and change mechanisms shall be governed by the applicable DPA, Main Agreement, or other applicable documents.

GloryScience's current list of material Sub-processors, including their service categories, processing purposes, and primary processing locations, will be published or made available through the Oneasy official website, administrative console, documentation pages, or other reasonable means. GloryScience will notify customers of any addition or replacement of a material Sub-processor that may have a material impact on the processing of Tenant Data in accordance with the applicable DPA, Main Agreement, or other applicable documents, and will provide a reasonable objection mechanism.

- **Legal Requirements:** We may disclose information to respond to valid legal processes, regulatory requirements, law enforcement requests, or court orders; to protect personal safety; to defend the lawful rights or property of us, our customers, or third parties; or where otherwise required by law.
- **Business Reorganization:** In connection with a merger, acquisition, financing, asset sale, business transfer, reorganization, or similar transaction, we may disclose relevant information to the extent necessary, while taking reasonable measures to ensure that your information remains subject to appropriate confidentiality and data protection obligations.

VII. Data Security

7.1 Security Standards

We will implement and maintain commercially reasonable technical and organizational security measures designed to protect personal information and Tenant Data from unauthorized access, disclosure, alteration, loss, or destruction. Such measures may include access controls, authentication, encryption in transit, protection of data at rest where applicable, logging and monitoring, vulnerability management, personnel confidentiality obligations, and incident response procedures.

Specific security controls, remote access security, Agent / VPN security, log retention, vulnerability management, security audit support, and technical and organizational measures shall be governed by the Oneasy Security Addendum, DPA, Main Agreement, or other security document separately agreed by the parties.

7.2 Security Incident Notification

If we confirm a security incident that may materially affect your personal information, Tenant Data, or the security of the Service, we will notify you without undue delay to the extent required by law. Where reasonably practicable and where preliminary confirmed information is available, we will generally provide customers with an initial notice within seventy-two (72) hours after confirming a material security incident.

The notice will, to the extent reasonably known to us, include the nature of the incident, the categories of data or systems affected, the known or likely impact, the control, mitigation, and remediation measures we have taken or are taking, the risk mitigation measures recommended for the customer, and follow-up communication channels. We may supplement such information as the investigation, forensic review, and remediation progress.

7.3 Backup and Recovery

We will implement reasonable data backup strategies in accordance with business needs and common industry practices. The specific backup frequency, retention period, recovery process, recovery time objective (RTO), and recovery point objective (RPO), if they constitute legally binding commitments, shall be governed by the applicable SLA, Order Form, Security Addendum, or special agreement separately signed or incorporated by the parties. Unless expressly agreed otherwise, RTO and RPO do not constitute legally binding service level commitments.

7.4 User Security Responsibilities

You understand and agree that the Internet, cloud services, and remote access environments are not absolutely secure environments. You must properly manage accounts, permissions, administrator identities, API keys, access tokens, VPN / Agent credentials, device credentials, network isolation policies, and internal approval processes.

Except where mandatory requirements of applicable law provide otherwise or where expressly agreed by the parties, we will not be liable for data leakage, network interruption, or losses arising from your failure to safeguard account credentials, improper operations by authorized users, improper permission configuration, insufficient network isolation on the customer side, vulnerabilities in customer-side devices or systems, failure to timely update Agent / VPN components, or your choice to access the Service through a network environment that does not meet security requirements. We strongly recommend that you enable multi-factor authentication (MFA) for administrator accounts, regularly review authorized users and permissions, and regularly rotate API keys, access tokens, and high-privilege credentials.

7.5 Data Retention

We retain personal information and Tenant Data only for as long as necessary to fulfill the purposes described in this Policy, the Main Agreement, applicable DPA, Security Addendum, or applicable law. The specific retention periods, deletion, anonymization, export, and exceptional retention rules for account information, Tenant Data,

operational logs, security logs, backup data, financial records, and dispute resolution materials shall be governed by the Main Agreement, applicable DPA, Security Addendum, system configuration, or applicable legal requirements.

VIII. Your Data Subject Rights

Depending on the data protection laws applicable to you, you may have the rights to access, correct, delete, restrict processing, obtain data portability, withdraw consent, and object to certain processing activities.

How to Exercise Your Rights: If you are an authorized user of a Tenant, please first contact your organization's account administrator. If you are the direct controller of the account, or if the administrator is unable to handle your request, please email support@oneasy.cc. For security reasons, we may verify your identity before processing your request.

For data subject requests relating to authorized users of a Tenant or to Tenant Data, the Tenant, as the controller or responsible party for the relevant data, shall process and respond to such requests in a timely manner in accordance with applicable law. GloryScience will assist the Tenant in fulfilling its applicable obligations within reasonable limits through the product features, APIs, export functions, or technical support of the Oneasy Service.

For personal information processed by GloryScience as controller, we will respond to verifiable requests within the time limits required by applicable law. To the extent permitted by applicable law, we may refuse or restrict requests that are manifestly unfounded, excessive, repetitive, affect the rights of others, involve trade secrets, create security risks, or involve information that is prohibited by law from disclosure.

IX. Disclaimer and Limitation of Liability

9.1 Service Provided "As Is"

To the maximum extent permitted by applicable law, our Service and all related content are provided on an "**as is**" and "**as available**" basis. Except for matters expressly committed to in the Main Agreement, DPA, Security Addendum, or other written agreement between the parties, we provide no express or implied warranties, including, without limitation, warranties of merchantability, fitness for a particular purpose, non-infringement, uninterrupted operation, or error-free operation. However, this section does not limit any liability of GloryScience arising from willful misconduct or gross negligence, or any liability that cannot be limited under applicable law.

9.2 Specific Exclusions

Except where mandatory requirements of applicable law provide otherwise or where expressly agreed by the parties, we will not be liable for any service interruption, delay, data loss, corruption, or inability to access caused directly or indirectly by any of the following:

1. Force majeure events beyond our control, such as natural disasters, war, civil unrest, large-scale cyberattacks, telecommunications backbone outages, major public cloud failures, or regulatory restrictions;
2. Your or your authorized users' operations, equipment failures, network connectivity issues, improper permission configurations, credential leakage, insufficient internal approvals, or failure to follow security recommendations;
3. Your failure to follow our service configuration guides, technical documentation, security recommendations, or reasonable operating procedures;
4. Planned or emergency maintenance conducted for reasonable system maintenance, upgrades, security fixes, or emergency risk remediation;

5. Any failure of third-party services, customer-side networks, customer equipment, device vendor firmware, private interfaces, third-party cloud services, or telecommunications service providers.

9.3 Allocation of Responsibility

The allocation of responsibility in relation to data processing, security incidents, or limitation of liability concerning the Oneasy Service shall be governed by the applicable Main Agreement, DPA, Security Addendum, and applicable law between GloryScience and the customer.

X. Governing Law, Dispute Resolution, and Independent Compliance Commitment

10.1 Governing Law

The interpretation, validity, and enforcement of this Policy, and any dispute arising out of this Policy, shall be governed by the laws of the Hong Kong Special Administrative Region, without regard to any conflict of law rules.

10.2 Compliance with Data Protection Laws

GloryScience will comply with the mandatory requirements imposed on it by applicable data protection laws, to the extent that such laws apply to GloryScience and have jurisdiction over the relevant processing activities, including, where applicable, the EU GDPR, UK GDPR, Hong Kong PDPO, Singapore PDPA, and other applicable laws. The foregoing shall not be interpreted as GloryScience unconditionally accepting the application of the laws of any jurisdiction that has no actual connection with the relevant processing activities.

Any conflict concerning governing law or dispute resolution shall remain subject to Section 10.1 of this Policy and the provisions of the Main Agreement. However, such provisions do not affect the ability of data subjects to lodge complaints with competent supervisory authorities or exercise non-waivable rights under applicable law.

10.3 Dispute Resolution

Any dispute arising out of or in connection with this Policy shall be handled in accordance with the dispute resolution mechanism set out in the Oneasy SaaS Service Agreement, including submission to arbitration administered by the Hong Kong International Arbitration Centre (HKIAC), if the Main Agreement adopts such mechanism. This arbitration provision does not affect the right of data subjects to lodge complaints with relevant supervisory authorities in accordance with law.

10.4 Policy Updates

We may revise this Policy from time to time. For material adverse changes, including a material expansion of the scope of personal information collected, new material sharing with third parties, a significant reduction in the standard of personal information protection, or changes that materially and adversely affect data subject rights, we will notify tenant administrators thirty (30) days in advance by email, administrative console notice, website announcement, or other reasonable means.

Where applicable law requires a shorter or longer notice period, or where security, legal, regulatory, service continuity, or emergency risk remediation considerations require faster effectiveness, we may handle the update in accordance with applicable law and reasonable commercial practices. Continued use of the Service after the updated policy becomes effective constitutes acceptance of the updated policy. If a user does not agree, the user should stop using the Service and may handle termination or data export matters in accordance with the Main Agreement.

XI. Contact Us

If you have any questions about this Policy or our privacy practices, please contact our data protection team through the following methods:

Legal and Data Protection Matters: legal@oneasy.cc

General Technical Support Matters: support@oneasy.cc

Postal Address: NEW TREND CTR, NO. 704 PRINCE EDWARD RD EAST, SAN PO KONG, HONG KONG