Oneasy Data Processing Agreement (DPA)

International Enterprise Edition

Last Updated: June 25, 2026
Effective Date: June 25, 2026

> This Agreement is a supplemental agreement to the Oneasy SaaS Service Agreement.
> This Agreement applies where GloryScience processes Personal Data on behalf of the Customer as a Processor through the Oneasy Services.
> If this Agreement conflicts with the Master Agreement, this Agreement shall prevail with respect to Personal Data Processing matters.

---

1. Parties and Scope

This Data Processing Agreement (the "**DPA**" or this "**Agreement**") is entered into by the following parties or applies by incorporation by reference:

1.1 Controller / Customer

The customer that accepts the Oneasy SaaS Service Agreement and uses the Oneasy Services.

1.2 Processor / GloryScience International Limited

GloryScience International Limited ("GloryScience")
Registered Address: **NEW TREND CTR, NO. 704 PRINCE EDWARD RD EAST, SAN PO KONG, HONG KONG**
Business Registration Number: **80032746**

1.3 Scope

This Agreement applies where GloryScience processes Personal Data on behalf of the Customer as a Processor, including Processing activities governed by:

- the EU GDPR;
- the UK GDPR;
- the Hong Kong PDPO;
- the Singapore PDPA; and
- other Applicable Data Protection Laws.

This Agreement does not apply where GloryScience processes data required for account administration, billing, payment, security, compliance, platform operations, service improvement, or statutory retention as an independent Controller, data user, organisation, or other functionally equivalent role. Such Processing activities shall be governed by the applicable Oneasy Privacy Policy, the Master Agreement, and Applicable Law.

1.4 Non-GDPR Jurisdictions

If Applicable Law does not use the terms "Controller / Processor," or if those terms have different meanings in the relevant jurisdiction, references in this Agreement to Controller / Processor shall be interpreted by reference to the roles, concepts, and obligations that are functionally closest under such law, including, without limitation, the concepts of data user / data processor under the Hong Kong PDPO and organisation / data intermediary under the Singapore PDPA. Such interpretation shall not expand GloryScience's statutory obligations beyond the scope expressly prescribed by Applicable Law.

1.5 Scope Limitation for Third-Party Technical Materials and Non-Personal Data Matters

This DPA governs only matters in which GloryScience processes Personal Data on behalf of the Customer as a Processor through the Oneasy Services. Third-Party Technical Materials, equipment-vendor materials, MIBs/OIDs, CLI/API materials, OMCI materials, firmware materials, configuration templates, scripts, packet-capture files, log samples, trade secrets, or other non-Personal Data materials submitted, uploaded, disclosed, provided, or authorized for use by the Customer through Oneasy are not governed by this DPA with respect to their source of rights, license to use, authorization for disclosure, confidentiality obligations, ownership of intellectual property, allocation of liability, or indemnification. Those matters shall instead be governed by the Oneasy SaaS Service Agreement, the Security Addendum, an Order Form, a SOW, or specific terms for technical materials separately agreed by the parties in writing.

For the avoidance of doubt, a particular item may contain both Personal Data and non-personal technical materials. The data protection obligations under this DPA apply only to the extent that such item constitutes Personal Data. This DPA shall not be interpreted as confirming that the Customer possesses a valid source of rights in any Third-Party Technical Materials, granting GloryScience a sufficient license to use third-party vendor materials, or requiring GloryScience to receive, copy, embed, distribute, sublicense, or continue using any materials that may be subject to third-party intellectual property rights, trade secrets, contractual restrictions, or confidentiality obligations.

The Customer's acceptance of the Oneasy SaaS Service Agreement, configuration of the Services, addition of devices, configuration of credentials, enablement of Agent / VPN / Connector / API / SNMP / TR-069 / TR-369 / CLI / Syslog / ACS / NMS interfaces, or uploading or submission of MIBs, OIDs, SNMP walk results, CLI/API outputs, configuration backups, logs, packet-capture files, scripts, templates, equipment materials, vendor materials, or other Third-Party Technical Materials may, to the extent involving Personal Data Processing, constitute the Customer's Processing instructions to GloryScience. However, the source of rights, authorization, license, confidentiality, and indemnification matters relating to the relevant non-personal technical materials shall continue to be governed by the Master Agreement, the Security Addendum, an Order Form, a SOW, or specific terms.

---

2. Definitions

Unless otherwise defined in this Agreement, the terms used in this Agreement shall have the same meanings as in the Oneasy SaaS Service Agreement.

2.1 Personal Data

"Personal Data" means any information relating to an identified or identifiable natural person.

2.2 Processing

"Processing" includes collection, recording, organization, storage, access, transmission, use, disclosure, restriction, deletion, destruction, analysis, and similar activities.

2.3 Customer Data

"Customer Data" means data uploaded, entered, generated, configured, authorized for reading, permitted to be generated, or otherwise processed through the Oneasy Services by or for the Customer, including, without limitation, network-device data, configuration data, log data, performance data, account data, support communications data, device outputs, SNMP walk results, CLI/API outputs, configuration backups, packet-capture files, diagnostic results, and other data generated by Customer devices, Customer networks, or Customer configurations. Customer Data is governed by the Personal Data pro-

tection provisions of this DPA only to the extent that it constitutes Personal Data. For non-Personal Data, Third-Party Technical Materials, equipment-vendor materials, or trade secrets, matters concerning the source of rights, licensing, confidentiality, and indemnification shall be governed by Section 1.5 and the relevant Master Agreement, Security Addendum, Order Form, SOW, or specific terms for technical materials.

2.4 Telecom Operational Data

"Telecom Operational Data" includes, without limitation:

- OLT / ONU identifiers;
- IP addresses;
- MAC addresses;
- network topology;
- configuration records;
- operation logs;
- telemetry;
- performance metrics; and
- fault and alarm records.

In certain jurisdictions, the above data may be regarded as Personal Data, regulated telecommunications data, communications metadata, network-security data, or data relating to critical infrastructure. The Customer shall independently assess the lawfulness of uploading, connecting, or Processing such data and shall bear the corresponding compliance responsibilities.

For the avoidance of doubt, Telecom Operational Data is a risk classification for data protection, communications regulation, and cybersecurity purposes. It does not automatically include, confirm, or authorize any non-public MIBs, private OIDs, CLI/API documentation, OMCI materials, firmware materials, proprietary protocol materials, or other Third-Party Technical Materials of any third-party vendor. Publicly released industry standards, public protocol specifications, public RFCs, public Broadband Forum technical reports, public data models, or public MIBs do not, merely because Oneasy supports, references, or implements them, automatically constitute confidential third-party materials. However, SNMP walk results, CLI/API outputs, configuration backups, packet captures, log samples, diagnostic results, or parsing results generated from Customer devices, Customer networks, or Customer configurations may simultaneously contain Personal Data, Customer network data, Third-Party Technical Materials, network-security-sensitive information, or regulated data. Ownership, authorization, confidentiality, and indemnification matters relating to such materials shall be handled in accordance with Section 1.5 and the relevant business agreements.

2.5 Restricted Transfer

"Restricted Transfer" means a transfer or access activity that, under the EU GDPR, UK GDPR, or other Applicable Data Protection Law, requires the application of Standard Contractual Clauses, a United Kingdom international data-transfer mechanism, a transfer impact assessment, or another lawful cross-border transfer mechanism because Personal Data is transferred to a country, territory, or international organization not recognized under the relevant law as providing adequate or equivalent protection.

2.6 Sensitive Data and Communications Content

Unless otherwise agreed by the parties in writing, the Customer shall not upload, connect, or process through the Oneasy Services any special categories of Personal Data, sensitive personal information, full payment-card data, health data, data concerning minors, government identity documents, communications content, unlawful surveillance data, unauthorized intercepted communications data, or other data for which Applicable Law requires a higher level of compliance protection.

3. Roles of the Parties

3.1 Customer as Controller

The Customer is the Controller of its Customer Data and any Personal Data contained therein, or assumes the functionally equivalent responsible role under Applicable Law. The Customer is responsible for:

- determining the purposes and means of Processing;
- confirming that the Processing has a lawful basis;
- obtaining necessary authorizations or consents;
- fulfilling notice obligations to Data Subjects;
- responding to Data Subject rights requests;
- ensuring that it has the right to access, upload, transmit, configure, manage, and process data relating to the relevant networks, devices, accounts, interfaces, logs, topology, subscribers, or end users;
- ensuring that its addition of devices, configuration of credentials, authorization to read device outputs, or uploading or permission to generate SNMP walk results, CLI/API outputs, configuration backups, packet captures, logs, diagnostic results, or other Customer Data has a lawful basis and constitutes a valid Processing instruction to the extent Personal Data is involved; and
- ensuring that its use of the Oneasy Services complies with Applicable Law.

3.2 GloryScience as Processor

GloryScience, as Processor, shall process Personal Data only on the Customer's lawful and documented instructions. GloryScience does not own Customer Data and will not use identifiable Customer Data for marketing, sale, or commercialization unrelated to the provision of the Services.

GloryScience's Processing of Customer Data shall not be interpreted as making GloryScience the operator or controller of the Customer's network, a managed network service provider, a telecommunications operator, a public communications service provider, a provider of communications services to the Customer's end users, or the party responsible for the Customer's non-transferable regulatory obligations.

3.3 Independent Controller Activities

With respect to account information, platform operational data, and necessary log data processed by GloryScience for account administration, billing, payment, security, compliance, service improvement, platform operations, fraud prevention, dispute handling, statutory retention, or necessary business records, GloryScience may process such data as an independent Controller or in a functionally equivalent role under Applicable Law and shall comply with Applicable Data Protection Law.

The Oneasy Privacy Policy, rather than this DPA, generally applies to the independent Controller activities described above. However, this DPA shall continue to apply to the same data to the extent GloryScience processes that data on behalf of the Customer through the Oneasy Services.

4. Processing Instructions

GloryScience shall process Personal Data only pursuant to the following documents or methods:

- the Oneasy SaaS Service Agreement;
- this DPA;
- an applicable Order Form / SOW;
- the Customer's configurations and operations within the Oneasy Services;
- in-Service instructions, including the Customer's addition of devices, configuration of credentials, enablement of Agent / VPN / Connector / API / SNMP / TR-069 / TR-369 / CLI / Syslog / ACS / NMS interfaces, uploading or

submission of files, authorization to read device outputs, or permission to generate SNMP walk results, CLI/API outputs, configuration backups, packet captures, logs, or diagnostic results;

- the Customer's written instructions; and
- requirements of Applicable Law.

If GloryScience considers that a Customer instruction manifestly violates Applicable Data Protection Law, communications secrecy law, cybersecurity law, sanctions or export-control requirements, or may create a material risk to Oneasy, the Customer, other customers, third-party systems, or network security, GloryScience may refuse, suspend, or defer execution of that instruction and shall notify the Customer to the extent reasonably practicable.

GloryScience may reasonably rely on Processing instructions and authorizations issued by the Customer through the Master Agreement, this DPA, the Security Addendum, an Order Form, a SOW, product configurations, in-Service operations, upload records, authorized-reading records, support tickets, or other documented means. Unless mandatorily required by Applicable Law or otherwise agreed by the parties in writing, GloryScience is not required, before each Processing operation involving Customer Data, device outputs, or Third-Party Technical Materials containing Personal Data, to separately verify the chain of authorization between the Customer and an equipment vendor, systems integrator, channel partner, end customer, end user, or other third party.

If Applicable Law requires GloryScience to process Personal Data without the Customer's instruction, GloryScience shall inform the Customer of that legal requirement before Processing, unless Applicable Law prohibits such notice on grounds of public interest, law enforcement, security, or confidentiality.

---

5. Categories of Data and Data Subjects

5.1 Categories of Personal Data

GloryScience may process the following categories of data on behalf of the Customer:

- names of Customer employees or Authorized Users;
- business email addresses;
- user accounts and role permissions;
- login records and access logs;
- IP addresses;
- device identifiers;
- telecommunications operation and maintenance logs;
- network configuration data;
- support communications records; and
- other data submitted or generated by the Customer through the Services.

5.2 Categories of Data Subjects

Data Subjects may include:

- Customer employees;
- Customer Authorized Users;
- operation and maintenance engineers;
- network administrators;
- the Customer's end users or subscribers, where the Customer connects relevant data to the Oneasy Services; and
- other natural persons associated with Customer Data.

5.3 Data Minimization and Restricted Data

The Customer shall submit to the Oneasy Services only data that is necessary, lawful, and appropriate for use of the Services. Unless otherwise agreed by the parties in writing, the Oneasy Services are not designed to store or process communications content, unlawful surveillance data, unauthorized intercepted communications data, special categories of Personal Data, sensitive personal information, or other highly sensitive data.

If the Customer believes that its use case unavoidably involves any of the foregoing data, the Customer shall notify Oneasy in writing before submitting such data and shall be responsible for determining whether additional local-law assessments, data protection impact assessments, communications-regulatory approvals, notices to subscribers or end users, consents, authorizations, filings, or other compliance measures are required. GloryScience may refuse to process such data for reasons of security, compliance, technical feasibility, or commercial risk.

---

6. Confidentiality

GloryScience shall ensure that persons authorized to access Personal Data are subject to appropriate confidentiality obligations. Except as necessary to provide the Services, comply with legal obligations, address a Security Incident, implement security and compliance measures, or as authorized by the Customer, GloryScience shall not disclose Customer Personal Data to unrelated persons.

---

7. Technical and Organizational Measures

GloryScience will implement technical and organizational security measures consistent with generally accepted industry practices to protect Personal Data against unauthorized or unlawful Processing and against accidental loss, destruction, or damage. Such measures shall be determined in light of the nature of the Processing activities, the types of data, the Processing risks, implementation costs, technical feasibility, and service-operational needs.

7.1 Access Control

GloryScience will use reasonable access-control measures through the Oneasy Services, including, without limitation:

- role-based access control (RBAC);
- the principle of least privilege;
- authentication controls;
- restrictions on administrative privileges; and
- internal access-approval processes.

7.2 Encryption

Within commercially reasonable limits, GloryScience will use the following through the Oneasy Services:

- encryption of data in transit;
- encryption of data at rest; and
- key-management measures.

7.3 Logging and Monitoring

GloryScience will maintain appropriate security logs and access records through the Oneasy Services for purposes including:

- security audits;
- anomaly detection;
- troubleshooting; and

- Security Incident response.

7.4 Vulnerability Management

GloryScience will implement reasonable vulnerability-management processes through the Oneasy Services according to business and security needs, including vulnerability scanning, security remediation, and risk assessment.

7.5 Backup and Recovery

GloryScience will implement reasonable data backup and recovery mechanisms through the Oneasy Services according to business needs. If specific backup cycles, retention periods, recovery time objectives (RTO), or recovery point objectives (RPO) are to constitute binding commitments, they must be set forth in a separately executed SLA or service order.

7.6 Security Assistance

To the extent required by Applicable Data Protection Law and where the Customer cannot obtain the relevant information independently through the functionality of the Oneasy Services, GloryScience will, taking into account the nature of the Processing, the information available to it, technical feasibility, and commercially reasonable standards, assist the Customer with reasonable requests relating to Personal Data security, data protection impact assessments, Security Incident assessments, and preparation for communications with regulators. Unless Applicable Law mandatorily requires otherwise or the parties otherwise agree in writing, the Customer shall bear reasonable fees for assistance beyond the scope of the standard Services.

---

8. Security Incident Notification

If GloryScience confirms a Security Incident that may have a material impact on Customer Data, Personal Data, or the security of the Services, GloryScience will notify the Customer as soon as reasonably practicable to the extent required by Applicable Law and without undue delay.

Where reasonably practicable and preliminary confirmed information is available, GloryScience will ordinarily provide the Customer with an initial notice within seventy-two (72) hours after confirming a material Security Incident. However, if the nature of the incident is complex, the investigation remains ongoing, or the law otherwise requires, GloryScience may supplement the notice in stages as further information becomes available.

To the extent reasonably known to GloryScience, the notice will include:

- the nature and basic circumstances of the Security Incident;
- the affected categories of data or scope of systems;
- known or potential impacts;
- containment, mitigation, and remediation measures taken or being taken by GloryScience;
- recommended risk-mitigation measures for the Customer; and
- a contact person or notification channel for further communications.

GloryScience may continue to supplement the relevant information as the investigation, forensic analysis, and response progress.

Where information is delayed, incomplete, or the investigation is constrained due to a third-party infrastructure provider, cloud service provider, network operator, Subprocessor, Customer environment, Customer network, Force Majeure Event, or legal restriction, GloryScience will use commercially reasonable efforts, within reasonable limits, to provide the relevant notices and updates.

---

9. Subprocessors

9.1 General Authorization

The Customer generally authorizes GloryScience to use Subprocessors in the course of providing the Services to assist with portions of the Services or data Processing activities, including, without limitation:

- cloud infrastructure providers;
- payment processors;
- customer-support system providers;
- security-monitoring and security-service providers;
- communications and notification providers;
- logging, analytics, and operation and maintenance tool providers; and
- AI service providers used when the Customer enables the relevant features.

9.2 Subprocessor Obligations

GloryScience shall take commercially reasonable measures to ensure that its Subprocessors undertake, through contracts or other binding arrangements, confidentiality, security, and data Processing responsibilities that are substantially equivalent to the data protection obligations under this Agreement, and that they process Personal Data only to the extent necessary to provide the relevant Services.

To the extent required by Applicable Data Protection Law, GloryScience shall remain liable to the Customer for the performance by its Subprocessors of the data protection obligations subcontracted to them. Such liability shall remain subject to the applicable limitations of liability in the Oneasy SaaS Service Agreement and this DPA, unless Applicable Law expressly prohibits such limitations.

9.3 Subprocessor List

GloryScience may provide a current list of material Subprocessors through its official website, administrative console, documentation pages, Customer notices, or other reasonable means. The list may identify the categories, purposes, types of Processing activities, and, to the extent commercially reasonable to disclose, Processing-location information for material Subprocessors.

For material Subprocessors supporting cloud infrastructure, AI services, logging and monitoring, security services, and customer support, the relevant list, service configuration, or applicable documentation may, within commercially reasonable limits, describe their primary cloud regions, support-access regions, AI-service invocation or model-related Processing locations, secondary nodes, disaster-recovery nodes, edge nodes, cache nodes, backup nodes, or other categories of Processing locations. Unless expressly stated otherwise in an applicable Order Form, DPA, Security Addendum, service configuration, Subprocessor list, or written agreement between the parties, such descriptions do not constitute an absolute commitment that Processing, storage, or data localization will occur within a particular jurisdiction.

9.4 Subprocessor Change Notice

If GloryScience adds or replaces a material Subprocessor that may materially affect the Processing of Customer Data, GloryScience will ordinarily notify the Customer at least thirty (30) days in advance by email, platform announcement, administrative-console notice, documentation-page update, or other reasonable means.

However, where a change involves security response, legal-compliance requirements, urgent infrastructure adjustments, service-continuity safeguards, a vendor service discontinuation, remediation of a material vulnerability, or another reasonably urgent circumstance, GloryScience may notify the Customer as soon as commercially reasonable after the change.

9.5 Customer Objection

If the Customer objects to a Subprocessor change on reasonable data protection or information-security grounds, the Customer shall submit the specific grounds for its objection in writing within thirty (30) days after receiving the notice. The parties shall negotiate in good faith to identify a reasonable solution.

If the parties cannot reach a solution within a reasonable period, the Customer may terminate the relevant Services directly affected by the Subprocessor change. The Customer shall not, however, be entitled on that basis to require GloryScience to bear liability for indirect loss, loss of anticipated profits, or other consequential loss beyond the unused service period.

9.6 Onward Transfer Controls

If a Subprocessor's Processing activities constitute a Restricted Transfer, GloryScience will, to the extent required by Applicable Law, take reasonable measures to ensure that the Subprocessor is subject to an applicable data-transfer mechanism, contractual obligations, or other lawful safeguards.

---

10. International Data Transfers

10.1 Processing Locations

By default, Customer Data is primarily stored in the Alibaba Cloud International Singapore region.

To provide the Services, disaster recovery, security protection, technical support, secondary-node access, log analysis, Subprocessor services, AI-assisted features, or to comply with legal obligations, relevant data may be accessed, processed, cached, backed up, or transferred in other jurisdictions.

For the avoidance of doubt, cross-border data Processing may include the following distinct scenarios:

- **Storage Location:** the primary cloud-hosting, primary-storage, or primary-backup location for Customer Data. By default, this is the Alibaba Cloud International Singapore region, unless otherwise expressly provided in an applicable Order Form, DPA, Security Addendum, service configuration, or written agreement between the parties;
- **Support Access Location:** the location from which GloryScience or its authorized personnel remotely access relevant data for support, security, operations and maintenance, implementation, troubleshooting, or service-continuity purposes;
- **Subprocessor Processing Location:** the location where a Subprocessor processes data in providing cloud infrastructure, support, monitoring, notifications, logging, payment, security, AI-assisted features, or other services; and
- **AI Service Invocation Location:** where the Customer has enabled AI-assisted features and they are applicable, relevant inputs, outputs, or contextual data may be invoked, transferred, cached, or processed in the Alibaba Cloud International Singapore region, at the relevant AI service provider or model-related Processing location, at a secondary node, edge node, cache node, or another necessary location.

GloryScience will take reasonable measures, according to service-operational needs, to manage risks associated with cross-border access to and Processing of data. Specific data regions, secondary nodes, Subprocessors, and Processing locations shall be determined by the applicable Order Form, DPA, Security Addendum, service configuration, Subprocessor list, or written agreement between the parties.

10.2 Transfer Mechanisms

Where required by Applicable Data Protection Law, GloryScience may support the use of applicable cross-border data-transfer mechanisms, including, without limitation:

- the European Commission Standard Contractual Clauses (the "**EU SCCs**");
- the UK International Data Transfer Addendum to the EU SCCs or the UK International Data Transfer Agreement (the "**UK IDTA**"); and
- other data-transfer mechanisms recognized under Applicable Law.

If the Customer or the relevant Personal Data is subject to the EU GDPR or UK GDPR, and Processing of such Personal Data by GloryScience or its Subprocessors constitutes a Restricted Transfer, the parties agree that the EU SCCs, UK Addendum, UK IDTA, or another applicable transfer mechanism shall apply to the extent required by Applicable Law. Unless otherwise agreed by the parties in writing:

- where the Customer, as Controller, transfers Personal Data to GloryScience, as Processor, EU SCCs Module 2 (Controller-to-Processor) shall apply;
- where the Customer, as Processor, transfers Personal Data to GloryScience, as Subprocessor, EU SCCs Module 3 (Processor-to-Processor) shall apply;
- for a Restricted Transfer subject to the UK GDPR, the mechanism under the UK Addendum or UK IDTA that corresponds to the relevant transfer structure shall apply;
- Section 1, Annex 1, and Annex 6 of this DPA constitute the relevant Processing description required for Annex I to the EU SCCs;
- Annex 2 of this DPA constitutes the description of technical and organizational measures required for Annex II to the EU SCCs; and
- Annex 3 of this DPA constitutes the Subprocessor description required for Annex III to the EU SCCs.

If Applicable Law, the Customer's review, or the contracting process requires the parties to execute, supplement, or update the EU SCCs, UK Addendum, UK IDTA, transfer impact assessment documentation, or other data-transfer documents separately, the parties shall reasonably cooperate to complete them. Except for mandatory provisions necessary for a Restricted Transfer, the limitations of liability, audit limitations, allocation of costs, Customer responsibilities, and service boundaries set forth in this DPA and the Oneasy SaaS Service Agreement shall continue to apply.

10.3 Security and Supplementary Measures

GloryScience will implement appropriate technical and organizational security measures, according to the nature of the Processing activities and reasonable commercial standards, to reduce risks associated with cross-border transfers of data.

Such measures may include:

- access controls and permission management;
- encryption of data in transit;
- security monitoring and log auditing;
- data segregation or the principle of minimum access;
- Subprocessor management; and
- reasonable security safeguards and risk-mitigation measures.

10.4 Customer Responsibility

As Controller, the party issuing data Processing instructions, or another responsible party for the relevant data, the Customer is responsible for:

- ensuring that it has a lawful basis for providing relevant data to GloryScience or permitting GloryScience to process it;
- fulfilling notice, disclosure, and consent obligations required by Applicable Law;
- completing a cross-border data transfer impact assessment (TIA / TRA) or other compliance assessment where applicable;
- confirming the lawfulness of transferring Personal Data, subscriber data, Telecom Operational Data, network-security data, or communications metadata to GloryScience and its Subprocessors; and
- ensuring that its use of the Services complies with the laws and regulations of its jurisdiction.

10.5 Compliance Cooperation

To the extent required by Applicable Law, the parties shall reasonably cooperate with each other as necessary to satisfy applicable data protection and cross-border data-transfer compliance requirements.

Unless expressly required by law or otherwise agreed by the parties in writing, GloryScience does not undertake to provide customized legal-compliance advice concerning the laws of any particular country or region, regulatory-compliance guarantees, data-localization commitments, government-access commitments, public-sector compliance commitments, or certifications for any particular industry.

11. Data Subject Requests

If GloryScience receives a Data Subject request relating to Customer Data, GloryScience may refer the request to the Customer for handling. The Customer, as Controller or the functionally equivalent responsible party under Applicable Law, is responsible for the final response to the Data Subject.

Within reasonable limits, GloryScience will assist the Customer through product functionality or technical support in fulfilling Data Subject rights requests, including requests for access, correction, deletion, restriction of Processing, data portability, or objection to Processing.

If the Customer requests assistance from GloryScience beyond the scope of standard service functionality or standard technical support, GloryScience may require the Customer to provide necessary information, verify the lawfulness of the request, confirm its scope, and bear reasonable assistance fees, unless Applicable Law mandatorily requires otherwise.

12. Deletion and Return of Data

After termination of the Services, the Customer may, within thirty (30) days and using the available functionality provided by the Oneasy Services, export, have returned, or migrate Customer Data. During that period, the Customer may also submit a written request that GloryScience delete or assist in returning specified Customer Data, but such request shall be subject to technical feasibility, account verification, security requirements, the status of data segregation, backup mechanisms, and restrictions under Applicable Law.

Unless the Customer submits a clear and executable request for return or deletion during the export period, GloryScience will complete the process of deleting Customer Data within ninety (90) days after termination of the Services.

The foregoing does not apply to backups, security logs, audit logs, system logs, data subject to statutory retention, billing records, data required for dispute resolution, fraud-prevention records, Security Incident records, or data required by GloryScience to protect its legitimate rights and interests or comply with legal obligations. Such data shall be segregated, access-restricted, or deleted in accordance with Oneasy's retention policies, Applicable Law, and security requirements.

Except as required by Applicable Law or as necessary for security, compliance, auditing, dispute resolution, billing, recordkeeping, fraud prevention, or protection of legitimate rights and interests, GloryScience will no longer actively process segregated Customer Data for commercial purposes.

13. Audit and Compliance

13.1 Documentation Review

The Customer may reasonably request that GloryScience provide explanatory documentation relating to data protection and security measures, compliance summaries, security-control overviews, summaries of technical and organizational measures (TOMs), responses to enterprise-customer security questionnaires, or summaries of third-party audit / certification reports, if available and disclosable. GloryScience may redact, summarize, or subject such materials to confidentiality restrictions in order to protect Oneasy, its customers, Subprocessors, suppliers, system security, and trade secrets.

13.2 Information Necessary to Demonstrate Compliance

To the extent required by Applicable Data Protection Law, GloryScience will provide information reasonably available to it that is necessary to demonstrate its compliance with its Processor obligations under this DPA. The provision of such information shall be subject to confidentiality obligations, information-security restrictions, protection of trade secrets, third-party confidentiality restrictions, protection of other customers' data, and reasonable limits on the scope of the request.

13.3 Audit Limits

Unless otherwise agreed by the parties in writing, neither Oneasy nor GloryScience is required to accept:

- unrestricted on-site audits;
- penetration testing that affects the security or stability of the Services;
- audits requiring disclosure of other customers' data, Oneasy trade secrets, source code, underlying infrastructure details, or highly sensitive security information;
- excessively frequent, disproportionate, or unreasonable audit requests; or
- audits that fail to comply with reasonable restrictions concerning notice, scope, confidentiality, fees, timing, personnel, tools, and security.

13.4 Enterprise Audit

For enterprise customers in highly regulated industries, the parties may separately agree on a reasonable audit scope, frequency, confidentiality obligations, cost allocation, and operating procedures.

Unless mandatorily required by Applicable Law or following a confirmed material Security Incident, a direct audit should ordinarily be limited to once every twelve (12) months and should be completed preferentially through document review, security questionnaires, summaries of third-party reports, explanatory meetings, or remote interviews. Any on-site audit, penetration test, scanning test, or highly sensitive security assessment requires GloryScience's prior written consent and must comply with Oneasy's security-testing rules and service-stability requirements.

---

14. AI Processing Restrictions

Unless expressly authorized by the Customer in writing, GloryScience will not:

- use identifiable Customer Data to train general-purpose artificial intelligence models;
- use Customer Data for AI commercialization purposes unrelated to providing the Services; or
- sell or rent Customer Data to third-party AI service providers.

AI outputs in the Oneasy Services are auxiliary recommendations only. The Customer shall not apply AI outputs directly to a production network environment without human review and confirmation.

If the Customer enables AI-assisted features, the Customer should avoid submitting Personal Data, communications content, sensitive personal information, sensitive subscriber data, or regulated data beyond what is necessary for those features. GloryScience may impose reasonable restrictions on AI-related data inputs, outputs, retention, invocation, or functional scope based on security, compliance, model-provider restrictions, or technical feasibility.

---

15. Telecom-Specific Compliance

The Customer understands and acknowledges that Customer Data may contain network topology, device configurations, operation and maintenance logs, IP addresses, MAC addresses, performance data, fault data, alarm data, subscriber-related identifiers, or other information relating to telecommunications operations and maintenance.

The Customer shall independently determine:

- whether it has the right to access, manage, and operate the relevant network devices;
- whether it has the right to submit the relevant data to the Oneasy Services;
- whether it has the right to authorize GloryScience and its Subprocessors to access, process, transmit, store, or analyze the relevant data through the Oneasy Services for purposes of providing the Services;
- whether authorization, filing, licensing, approval, or consent is required under local telecommunications-regulatory law, communications-secrecy law, cybersecurity law, critical-infrastructure law, or data protection law; and
- whether the data involves end-user communications data, subscriber data, communications content, or regulated communications metadata.

The Customer shall not upload, process, or store through the Oneasy Services any unlawful surveillance data, unauthorized intercepted communications data, communications content, data that violates Applicable communications-secrecy law, or subscriber, end-user, or third-party data for which proper authorization has not been obtained.

The Oneasy Services provide a SaaS platform, network OAM assistance, technical support, diagnostics, analysis, recommendations, workflows, or automation-assistance capabilities. They do not make GloryScience the operator of the Customer's network, a telecommunications operator, a public communications service provider, a service provider to the Customer's end users, or the party responsible for the Customer's regulatory obligations.

16. Liability

The limitations of liability under this DPA are governed by Section 9 of the Oneasy SaaS Service Agreement. If Applicable Law expressly prohibits limiting a particular category of liability, the limitations of liability shall not apply to the extent such limitation is prohibited by that law.

For the avoidance of doubt, unless Applicable Law expressly prohibits limitation or the parties otherwise agree in writing, GloryScience shall not be liable beyond the limitations of liability in the Master Agreement for losses arising from the Customer's unlawful uploading or Processing of data, the Customer's failure to obtain necessary authorization or consent, the Customer's network or device environment, Customer configuration errors, the Customer's failure to fulfill local communications or data protection compliance obligations, third-party devices or services, Force Majeure Events, or the Customer's direct application of AI outputs to a production network without human review.

17. Governing Law and Disputes

This DPA is governed by the laws of the Hong Kong Special Administrative Region.

Any dispute arising out of or relating to this DPA shall be handled in accordance with the dispute-resolution mechanism set forth in Section 12 of the Oneasy SaaS Service Agreement.

18. Order of Precedence

If there is a conflict among different documents, the following order of precedence shall apply unless the parties expressly agree otherwise through an Order Form, SOW, Enterprise SLA, or other authorized written document:

1. Order Form / Subscription Order / SOW / Enterprise SLA;
2. Data Processing Agreement / DPA;
3. Security Addendum;
4. Oneasy SaaS Service Agreement;

5. Oneasy Payment and Refund Terms;
6. Oneasy Privacy Policy;
7. Oneasy Cookie Policy; and
8. Oneasy Website Terms of Use.

However, the Payment and Refund Terms shall prevail with respect to matters exclusively concerning payment, refunds, billing, automatic renewal, chargebacks, and late payment; the Website Terms of Use shall prevail with respect to access to the public website; the Cookie Policy shall prevail with respect to Cookies and tracking technologies; the DPA shall prevail with respect to Personal Data Processing; and the Security Addendum shall prevail with respect to security controls. If a security matter also concerns Personal Data Processing, cross-border transfers, notification of a Personal Data Breach, or obligations under Data Protection Law, the DPA shall prevail.

Annex 1 - Processing Description

Item	Description
Subject Matter	Provision of Oneasy SaaS telecom operations, network OAM assistance, diagnostics, monitoring, support, analytics and related platform services
Nature of Processing	Hosting, storage, access, transmission, monitoring, analytics, support, troubleshooting, security operations, backup, deletion, return and service improvement
Purpose of Processing	To provide, maintain, secure, troubleshoot, support and improve Oneasy services for customer
Duration	Subscription term plus applicable retention, export, backup, legal, security, audit and dispute-resolution periods
Categories of Data	Account data, user identifiers, device identifiers, IP addresses, MAC addresses, telecom operational data, logs, configuration data, support communications, telemetry, performance metrics, fault and alarm records
Categories of Data Subjects	Customer employees, authorized users, network administrators, operation engineers, customer contractors, end users or subscribers where customer lawfully submits or enables processing of such data
Sensitive Data / Communications Content	Not intended for processing unless expressly agreed in writing; customer must not submit special category data, sensitive personal information, communications content, illegal interception data or unauthorized subscriber / end-user data
Processing Frequency	Continuous or recurring as necessary to provide the services, and occasional for support, security, incident response, troubleshooting, migration, backup, deletion or compliance purposes
Processing Location	Primarily Alibaba Cloud International Singapore region, with limited cross-border storage, access or processing in other regions as necessary for redundancy, support, security, disaster recovery, subprocessors, AI-assisted features where enabled, edge access, or legal compliance
Controller Responsibilities	Customer determines processing purposes and means, maintains lawful basis, provides required notices, obtains consents or authorizations, responds to data subject requests, and confirms lawful authority over networks, systems, devices, accounts, interfaces and data submitted to Oneasy
Processor Responsibilities	GloryScience processes personal data through Oneasy services only on documented instructions, implements commercially reasonable TOMs, manages subprocessors, assists with data subject requests and security obligations as required by this DPA and applicable law, and deletes or returns data as described in this DPA

Annex 2 - Technical and Organizational Measures (TOMs)

GloryScience maintains commercially reasonable security controls for Oneasy services including:

- Role-based access control;
- Least privilege access;
- Authentication controls;
- Administrative access restrictions;
- Internal access approval processes;
- Encryption in transit;
- Encryption at rest where applicable;
- Access logging;
- Security monitoring;
- Vulnerability management;
- Backup management;
- Incident response procedures;
- Confidentiality obligations for personnel;
- Subprocessor management;
- Customer data segregation controls;
- Data minimization and purpose limitation controls where technically feasible;
- Secure deletion or data isolation procedures where applicable;
- Reasonable controls for support access and remote operational access where relevant.

Specific technical details may vary by service plan, deployment model, customer configuration, subprocessor service, feature enablement and technical feasibility. Any service-level commitment, RTO, RPO, dedicated environment, data localization, customized encryption, customer-managed keys, penetration testing, regulated-customer control, or enhanced security control must be expressly agreed in an Order Form, SOW, SLA, Security Addendum or other written agreement.

Annex 3 - Subprocessor Categories

GloryScience may use subprocessors in the following categories:

Category	Purpose
Cloud Infrastructure Provider	Hosting, storage, compute, networking, backup, disaster recovery
Payment Processor	Payment authorization, settlement, invoicing support, fraud prevention
Customer Support Tool	Support tickets, customer communications, troubleshooting records
Monitoring and Logging Tool	Security monitoring, diagnostics, service reliability, incident response
Communication Provider	Email, notification and service alerts
AI Service Provider	AI-assisted analysis where enabled and subject to applicable restrictions
Security Service Provider	Security monitoring, vulnerability management, threat detection, incident response support

A detailed subprocessor list may be published separately, made available through a documentation page or provided upon reasonable request, subject to security, confidentiality and commercial limitations.

Annex 4 - Telecom Operational Data Notice

Customer acknowledges that telecom operational data may be sensitive in certain jurisdictions. Depending on the applicable law, such data may be treated as:

- personal data;
- regulated telecom data;
- communications metadata;
- network security data;
- subscriber-related data;
- critical infrastructure related data.

Customer remains responsible for determining whether its use of Oneasy requires additional notices, consents, licenses, filings, approvals, authorizations or contractual arrangements under applicable telecom, cybersecurity, data protection, communications secrecy, critical infrastructure or sector-specific laws.

Customer must not use Oneasy services to upload, store, analyze or process unlawful interception data, unauthorized communications content, communications content not necessary for the services, or regulated subscriber / end-user data for which customer lacks required authority, notice, consent or legal basis.

GloryScience's receipt, processing, analysis or support access to telecom operational data through Oneasy services does not make GloryScience a telecom carrier, ISP, public communications service provider, managed network operator, operator of customer's production network, or legal responsible party for customer's licenses, regulatory filings, subscriber notices, end-user communications secrecy obligations or public-service continuity obligations.

Annex 5 - GDPR Article 28 Mapping

This Annex is provided for customer legal review convenience and should be read together with the full DPA.

GDPR Article 28 Requirement	DPA Coverage
Processing on documented instructions	Sections 3.2 and 4
Subject matter, duration, nature and purpose of processing	Annex 1
Type of personal data and categories of data subjects	Section 5 and Annex 1
Controller rights and obligations	Sections 3.1, 10.4, 11, 12 and Annex 1
Confidentiality of authorized personnel	Section 6 and Annex 2
Security measures under Article 32	Section 7 and Annex 2
Subprocessor authorization and change notice	Sections 9.1, 9.3, 9.4 and 9.5
Subprocessor flow-down obligations	Sections 9.2 and 9.6
Assistance with data subject rights	Section 11
Assistance with security, breach, DPIA and consultation obligations	Sections 7.6, 8, 10.5 and 13
Deletion or return after end of processing	Section 12
Information necessary to demonstrate compliance	Sections 13.1 and 13.2
Audit and inspection mechanism subject to reasonable limits	Sections 13.3 and 13.4
International transfer safeguards where applicable	Section 10 and Annex 6

Annex 6 - Cross-Border Transfer and Data Flow Summary

Data Flow / Processing Scenario	Typical Location / Role	Purpose	Safeguards / Notes
Primary hosting and storage	Primarily Alibaba Cloud International Singapore region, unless another location is specified in the applicable Order Form, service documentation, Security Addendum or written agreement	SaaS platform hosting, storage, backup, service delivery	Access controls, encryption where applicable, logging, subprocessor management
Remote support access	GloryScience authorized personnel or support resources may access from relevant support locations, including Singapore or other regions where support resources or access nodes are located	Troubleshooting, support, implementation, security, service reliability	Least privilege, access logging, confidentiality, purpose limitation
Cloud infrastructure processing	Alibaba Cloud International Singapore region as the primary cloud infrastructure region; other regions may be used for redundancy, edge access, backup, disaster recovery, support or compliance	Hosting, storage, compute, networking, backup, disaster recovery	Subprocessor contractual controls, security controls, transfer mechanism where required
Monitoring and logging	Singapore primary region or relevant monitoring, logging and security subprocessor locations, as necessary for diagnostics, security, incident response or service reliability	Security monitoring, diagnostics, incident response, service reliability	Data minimization where feasible, access controls, logging, contractual controls
Customer support tools	Relevant support and ticketing subprocessor locations	Customer communication, issue tracking, technical support	Confidentiality, access controls, limited support data processing
AI-assisted features where enabled	Alibaba Cloud International Singapore region, relevant AI service provider or model-related processing locations, or other regions necessary for enabled AI-assisted features	AI-assisted diagnostics, recommendations, analysis or workflow support	Customer enablement or authorization where applicable, no training of general AI models using identifiable customer data unless expressly authorized, input minimization, AI restrictions under Section 14
Payment processing	Payment processor locations	Payment authorization, settlement, invoicing support, fraud prevention	Payment processor terms, limited billing/payment data, PCI or payment compliance handled by relevant payment processor where applicable
Legal or compliance processing	Locations required by applicable legal process or compliance obligations	Legal compliance, dispute resolution, fraud prevention, regulatory response	Limited disclosure, legal review, access restriction where feasible

Where a Restricted Transfer arises, the mechanisms described in Section 10.2 apply to the extent required by applicable law. This Annex is intended to support customer review, security questionnaires, transfer impact assessments and data-mapping discussions, but does not constitute a data localization commitment or a guarantee that all processing will occur only in a specified jurisdiction unless expressly agreed in writing.

Note: The "Singapore region" refers to the primary cloud hosting, primary data processing, and primary storage region for the Oneasy services. Hong Kong is the place of incorporation and the location of the contracting entity and governing jurisdiction of GloryScience International Limited, and shall not be interpreted as the default primary storage region for the Oneasy services unless otherwise expressly specified in the applicable Order Form, DPA, Security Addendum, service configuration, subprocessor list, or written agreement between the parties.

Note: "Payment processing service provider" primarily applies where GloryScience processes billing/payment data as an independent controller; it constitutes a subprocessor only when it processes personal data within the scope of the DPA on behalf of the customer.