Oneasy Data Processing Agreement (DPA)

Oneasy 数据处理协议（国际企业版）

最后更新日期： 2026年6月25日
生效日期： 2026年6月25日

> 本协议为《Oneasy SaaS 服务协议》的补充协议。
> 本协议适用于 GloryScience 通过 Oneasy 服务作为数据处理者（Processor）代表客户处理个人数据的情形。
> 若本协议与主协议存在冲突，则就个人数据处理事项而言，以本协议为准。

---

1. Parties and Scope

第一条 双方与适用范围

本《Data Processing Agreement》（“**DPA**”或“**本协议**”）由以下双方签署或通过引用方式适用：

1.1 Controller / Customer（数据控制者 / 客户）

即接受《Oneasy SaaS 服务协议》并使用 Oneasy 服务的客户。

1.2 Processor / GloryScience International Limited（数据处理者 / GloryScience International Limited）

GloryScience International Limited（简称 GloryScience）
注册地址：**NEW TREND CTR, NO. 704 PRINCE EDWARD RD EAST, SAN PO KONG, HONG KONG**
商业登记证编号：**80032746**

1.3 Scope（适用范围）

本协议适用于 GloryScience 作为数据处理者代表客户处理个人数据的情形，包括受以下法律规制的处理活动：

- EU GDPR；
- UK GDPR；
- Hong Kong PDPO；
- Singapore PDPA；
- 以及其他适用的数据保护法律。

本协议不适用于 GloryScience 以独立数据控制者、数据使用者、组织或其他功能上相当角色处理账户管理、账单、支付、安全、合规、平台运营、服务改进或法定留存所需数据的情形；该等处理活动应按照 Oneasy 适用的隐私政策、主协议及适用法律处理。

1.4 Non-GDPR Jurisdictions（非 GDPR 法域解释）

如适用法律未使用 “Controller / Processor” 术语，或该等术语在相关法域下具有不同含义，本协议中关于 Controller / Processor 的表述应按该法律下功能上最接近的角色、概念和义务解释，包括但不限于 Hong Kong PDPO 下的 data user / data processor 概念及 Singapore PDPA 下的 organisation / data intermediary 概念。该等解释不应扩大 GloryScience 在适用法律未明确规定范围之外的法定义务。

1.5 Scope Limitation for Third-Party Technical Materials（第三方技术资料及非个人数据事项排除）

本 DPA 仅规范 GloryScience 通过 Oneasy 服务作为数据处理者代表客户处理个人数据的事项。客户通过 Oneasy 提交、上传、披露、提供或授权使用的第三方技术资料、设备厂商资料、MIB/OID、CLI/API、OMCI、固件资料、配置模板、脚本、抓包文件、日志样本、商业秘密或其他非个人数据资料，其权利来源、使用许可、披露授权、保密义务、知识产权归属、责任承担和赔偿事项，不由本 DPA 调整，应以《Oneasy SaaS 服务协议》、Security Addendum、Order Form、SOW 或双方另行书面约定的专项技术资料条款为准。

为避免疑义，某项资料可能同时包含个人数据和非个人技术资料。本 DPA 仅在该等资料构成个人数据的范围内适用数据保护义务；本 DPA 不应被解释为确认客户拥有任何第三方技术资料的权利来源、授予 GloryScience 使用第三方厂商资料的充分许可，或要求 GloryScience 接收、复制、内置、分发、转授权或继续使用任何可能受第三方知识产权、商业秘密、合同限制或保密义务约束的资料。

客户接受《Oneasy SaaS 服务协议》、配置服务、添加设备、配置凭据、启用 Agent / VPN / Connector / API / SNMP / TR-069 / TR-369 / CLI / Syslog / ACS / NMS 接口、上传或提交 MIB、OID、SNMP walk 结果、CLI/API 输出、配置备份、日志、抓包文件、脚本、模板、设备资料、厂商资料或其他第三方技术资料的行为，可在个人数据处理范围内构成客户对 GloryScience 的处理指令；但相关非个人技术资料的权利来源、授权、许可、保密和赔偿事项仍应按主协议、Security Addendum、Order Form、SOW 或专项条款处理。

---

2. Definitions

第二条 定义

除本协议另有定义外，本协议中的术语与《Oneasy SaaS 服务协议》保持一致。

2.1 Personal Data（个人数据）

“个人数据”指任何与已识别或可识别自然人相关的信息。

2.2 Processing（处理）

“处理”包括收集、记录、组织、存储、访问、传输、使用、披露、限制、删除、销毁、分析等行为。

2.3 Customer Data（客户数据）

“客户数据”指客户上传、输入、生成、配置、授权读取、允许生成或通过 Oneasy 服务处理的数据，包括但不限于网络设备数据、配置数据、日志数据、性能数据、账号数据、支持沟通数据、设备输出结果、SNMP walk 结果、CLI/API 输出、配置备份、抓包文件、诊断结果及其他由客户设备、客户网络或客户配置产生的数据。客户数据仅在其构成个人数据的范围内受本 DPA 的个人数据保护条款调整；非个人数据、第三方技术资料、设备厂商资料或商业秘密相关的权利来源、许可、保密与赔偿事项，适用第 1.5 条及相关主协议、Security Addendum、Order Form、SOW 或专项技术资料条款。

2.4 Telecom Operational Data（电信运维数据）

“Telecom Operational Data” 包括但不限于：

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

在部分法域中，上述数据可能被认定为个人数据、受监管的电信数据、通信元数据、网络安全数据或关键基础设施相关数据。客户应自行评估其上传、接入或处理相关数据的合法性，并承担相应合规责任。

为避免疑义，Telecom Operational Data 是数据保护、通信监管和网络安全风险分类，并不当然涵盖、确认或授权任何第三方厂商的非公开 MIB、私有 OID、CLI/API 文档、OMCI 资料、固件资料、专有协议资料或其他第三方技术资料。公开发布的行业标准、公开协议规范、公开 RFC、公开 Broadband Forum 技术报告、公开数据模型或公开 MIB，本身不因 Oneasy 支持、引用或实现而当然构成第三方保密资料；但基于客户设备、客户网络或客户配置生成的 SNMP walk 结果、CLI/API 输出、配置备份、抓包、日志样本、诊断结果或解析结果，仍可能同时包含个人数据、客户网络数据、第三方技术资料、网络安全敏感信息或受监管数据。该等资料的权属、授权、保密与赔偿问题按照第 1.5 条及相关业务协议处理。

2.5 Restricted Transfer（受限跨境传输）

“Restricted Transfer” 指根据 EU GDPR、UK GDPR 或其他适用数据保护法律，因个人数据被转移至未被相关法律认可为充分保护或等同保护的国家、地区或国际组织，而需要适用标准合同条款、英国国际数据传输机制、转移影响评估或其他合法跨境传输机制的传输或访问活动。

2.6 Sensitive Data and Communications Content（敏感数据与通信内容）

除双方另有书面约定外，客户不得通过 Oneasy 服务上传、接入或处理特殊类别个人数据、敏感个人信息、支付卡完整数据、健康数据、未成年人数据、政府身份识别文件、通信内容、非法监听数据、未授权通信截获数据，或其他适用法律要求更高合规保护等级的数据。

---

3. Roles of the Parties

第三条 双方角色

3.1 Customer as Controller（客户作为数据控制者）

客户为其客户数据及其中包含的个人数据的数据控制者，或在适用法律下承担功能上相当的责任角色。客户负责：

- 确定处理目的和方式；
- 确认数据处理具有合法基础；
- 获得必要授权或同意；
- 履行数据主体告知义务；
- 响应数据主体权利请求；
- 确保其有权接入、上传、传输、配置、管理和处理相关网络、设备、账户、接口、日志、拓扑、订户或终端用户相关数据；
- 确保其添加设备、配置凭据、授权读取设备输出、上传或允许生成 SNMP walk 结果、CLI/API 输出、配置备份、抓包、日志、诊断结果或其他客户数据的行为具有合法依据，并在个人数据范围内构成有效处理指令；
- 确保其使用 Oneasy 服务的行为符合适用法律。

3.2 GloryScience as Processor（GloryScience 作为数据处理者）

GloryScience 作为数据处理者，仅根据客户的合法、记录化指示处理个人数据。GloryScience 不拥有客户数据的所有权，也不会将可识别的客户数据用于与提供服务无关的营销、出售或商业化目的。

GloryScience 对客户数据的处理不应被解释为 GloryScience 成为客户网络的运营者、控制者、托管网络服务提供商、电信运营商、公共通信服务提供者、客户终端用户通信服务提供者或客户不可转移监管义务的承担方。

3.3 Independent Controller Activities（独立控制者活动）

对于 GloryScience 为账户管理、账单、支付、安全、合规、服务改进、平台运营、欺诈防控、争议处理、法定留存或必要业务记录目的处理的账户信息、平台运行数据和必要日志数据，GloryScience 可作为独立数据控制者或适用法律下功能上相当的角色处理该等数据，并应遵守适用的数据保护法律。

上述独立控制者活动通常适用 Oneasy 的隐私政策，而非本 DPA；但同一数据在 GloryScience 通过 Oneasy 服务代表客户处理的范围内，仍适用本 DPA。

---

4. Processing Instructions

第四条 处理指令

GloryScience 仅根据以下文件或方式处理个人数据：

- 《Oneasy SaaS 服务协议》；
- 本 DPA；
- 适用的 Order Form / SOW；
- 客户在 Oneasy 服务内的配置和操作；
- 客户添加设备、配置凭据、启用 Agent / VPN / Connector / API / SNMP / TR-069 / TR-369 / CLI / Syslog / ACS / NMS 接口、上传或提交文件、授权读取设备输出、允许生成 SNMP walk 结果、CLI/API 输出、配置备份、抓包、日志或诊断结果等服务内指令；
- 客户的书面指令；
- 适用法律要求。

若 GloryScience 认为某项客户指令明显违反适用数据保护法律、通信保密法律、网络安全法律、制裁或出口管制要求、或可能对 Oneasy、客户、其他客户、第三方系统或网络安全产生重大风险，GloryScience 有权拒绝、暂停或延后执行该指令，并在合理可行范围内通知客户。

GloryScience 有权合理依赖客户在主协议、本 DPA、Security Addendum、Order Form、SOW、产品配置、服务内操作、上传记录、授权读取记录、工单或其他记录化方式中作出的处理指令和授权。除适用法律强制要求或双方另有书面约定外，GloryScience 无义务在每次处理客户数据、设备输出结果或含个人数据的第三方技术资料前单独核查客户与设备厂商、系统集成商、渠道伙伴、终端客户、最终用户或其他第三方之间的授权链条。

若适用法律要求 GloryScience 在未获客户指示的情况下处理个人数据，GloryScience 应在处理前通知客户相关法律要求，除非适用法律基于公共利益、执法、安全或保密原因禁止该等通知。

---

5. Categories of Data and Data Subjects

第五条 数据类别与数据主体

5.1 Categories of Personal Data（个人数据类别）

GloryScience 可能代表客户处理以下类别的数据：

- 客户员工或授权用户姓名；
- 工作邮箱；
- 用户账号与角色权限；
- 登录记录与访问日志；
- IP 地址；
- 设备标识符；
- 电信运维日志；
- 网络配置数据；
- 支持沟通记录；
- 其他由客户通过服务提交或生成的数据。

5.2 Categories of Data Subjects（数据主体类别）

数据主体可能包括：

- 客户员工；
- 客户授权用户；
- 运维工程师；
- 网络管理员；
- 客户的最终用户或订户（如客户将相关数据接入 Oneasy 服务）；
- 其他与客户数据相关的自然人。

5.3 Data Minimization and Restricted Data（数据最小化与限制性数据）

客户应仅向 Oneasy 服务提交为使用服务所必要、合法且适当的数据。除双方另有书面约定外，Oneasy 服务并非设计用于存储或处理通信内容、非法监听数据、未授权通信截获数据、特殊类别个人数据、敏感个人信息或其他高敏感数据。

如客户认为其使用场景不可避免涉及上述数据，客户应在提交相关数据前书面通知 Oneasy，并负责确认是否需要额外的本地法律评估、数据保护影响评估、通信监管审批、订户或最终用户告知、同意、授权、备案或其他合规措施。GloryScience 可基于安全、合规、技术可行性或商业风险理由拒绝处理该等数据。

---

6. Confidentiality

第六条 保密义务

GloryScience 应确保被授权访问个人数据的人员受到适当保密义务约束。除为提供服务、履行法律义务、处理安全事件、实施安全和合规措施或获得客户授权外，GloryScience 不得向无关人员披露客户个人数据。

---

7. Technical and Organizational Measures

第七条 技术与组织安全措施

GloryScience 将实施符合行业通行实践的技术与组织安全措施，以保护个人数据免遭未经授权或非法处理、意外丢失、毁损或损坏。该等措施应结合处理活动性质、数据类型、处理风险、实施成本、技术可行性和服务运营需要确定。

7.1 Access Control（访问控制）

GloryScience 将通过 Oneasy 服务采用合理的访问控制措施，包括但不限于：

- RBAC；
- 最小权限原则；
- 身份认证控制；
- 管理员权限限制；
- 内部访问审批流程。

7.2 Encryption（加密）

GloryScience 将通过 Oneasy 服务在商业合理范围内采用：

- 传输中数据加密；
- 静态数据加密；
- 密钥管理措施。

7.3 Logging and Monitoring（日志与监控）

GloryScience 将通过 Oneasy 服务维护适当的安全日志和访问记录，用于：

- 安全审计；
- 异常检测；
- 故障排查；
- 安全事件响应。

7.4 Vulnerability Management（漏洞管理）

GloryScience 将根据业务和安全需要，通过 Oneasy 服务实施合理的漏洞管理流程，包括漏洞扫描、安全修复和风险评估。

7.5 Backup and Recovery（备份与恢复）

GloryScience 将根据业务需要，通过 Oneasy 服务实施合理的数据备份和恢复机制。具体备份周期、保留期限、RTO、RPO 如构成具有约束力的承诺，应以双方另行签署的 SLA 或服务订单为准。

7.6 Security Assistance（安全合规协助）

在适用数据保护法律要求且客户无法自行通过 Oneasy 服务功能获得相关信息的范围内，GloryScience 将根据处理活动性质、可获得信息、技术可行性及商业合理标准，协助客户履行与个人数据安全、数据保护影响评估、安全事件评估及监管沟通准备相关的合理请求。除适用法律另有强制要求或双方另有书面约定外，客户应承担超出标准服务范围的合理协助费用。

---

8. Security Incident Notification

第八条 安全事件通知

若 GloryScience 确认发生可能对客户数据、个人数据或服务安全产生重大影响的安全事件，GloryScience 将在适用法律要求范围内，且在合理可行情况下尽快通知客户，不应无故拖延。

在合理可行且具备初步确认信息的情况下，GloryScience 通常将在确认重大安全事件后七十二（72）小时内向客户发出初步通知；但如事件性质复杂、仍处于调查阶段，或法律另有要求，GloryScience 可在获得进一步信息后分阶段补充通知内容。

通知内容将在 GloryScience 合理掌握信息的范围内包括：

- 安全事件的性质及基本情况；
- 受影响的数据类别或系统范围；
- 已知或可能产生的影响；
- GloryScience 已采取或正在采取的控制、缓解及修复措施；
- 建议客户采取的风险缓解措施；
- 后续沟通联系人或通知渠道。

GloryScience 可根据事件调查、取证及处置进展，持续补充相关信息。

对于因第三方基础设施服务商、云服务提供商、网络运营商、子处理者、客户环境、客户网络、不可抗力或法律限制导致的信息延迟、不完整或调查受限情况，GloryScience 将在合理范围内尽商业合理努力提供相关通知与更新。

---

9. Subprocessors

第九条 子处理者

9.1 General Authorization（一般授权）

客户一般性授权 GloryScience 在提供服务过程中使用子处理者协助履行部分服务或数据处理活动，包括但不限于：

- 云基础设施服务商；

- 支付处理服务商；
- 客户支持系统服务商；
- 安全监控与安全服务提供商；
- 通信与通知服务商；
- 日志、分析及运维工具服务商；
- 在客户启用相关功能时使用的 AI 服务提供商。

9.2 Subprocessor Obligations（子处理者义务）

GloryScience 应采取商业上合理的措施，确保其子处理者通过合同或其他具有约束力的安排承担与本协议项下数据保护义务实质相当的保密、安全和数据处理责任，且仅在为提供相关服务所必要的范围内处理个人数据。

在适用数据保护法律要求的范围内，GloryScience 对其子处理者履行已分包数据保护义务的行为向客户承担责任；但该等责任仍受《Oneasy SaaS 服务协议》及本 DPA 中适用的责任限制约束，除非适用法律明确禁止该等限制。

9.3 Subprocessor List（子处理者清单）

GloryScience 可通过官方网站、管理后台、文档页面、客户通知或其他合理方式提供当前重要子处理者清单。该清单可列明重要子处理者的类别、用途、处理活动类型及在商业合理范围内可披露的处理地点信息。

对于云基础设施、AI 服务、日志监控、安全服务和客户支持等重要子处理者，相关清单、服务配置或适用文件可在商业合理范围内说明其主云区域、支持访问区域、AI 服务调用或模型相关处理地点、从节点、灾备节点、边缘节点、缓存节点、备份节点或其他处理地点类别。除适用的 Order Form、DPA、Security Addendum、服务配置、子处理者清单或双方书面约定另有明确规定外，该等说明不构成特定司法辖区内处理、存储或数据本地化的绝对承诺。

9.4 Subprocessor Change Notice（子处理者变更通知）

如 GloryScience 新增或更换可能对客户数据处理产生重大影响的重要子处理者，GloryScience 通常将提前至少三十（30）日通过电子邮件、平台公告、管理后台通知、文档页面更新或其他合理方式通知客户。

但在涉及安全响应、法律合规要求、紧急基础设施调整、服务连续性保障、供应商停服、重大漏洞修复或其他合理紧急情形下，GloryScience 可在变更后尽商业合理努力尽快通知客户。

9.5 Customer Objection（客户异议）

客户如基于合理的数据保护或信息安全理由反对子处理者变更，应在收到通知后三十（30）日内书面提出具体异议理由。双方应本着善意原则协商合理解决方案。

如双方无法在合理期限内达成解决方案，客户可终止受该子处理者变更直接影响的相关服务；但客户无权因此要求 GloryScience 对未使用期间之外的间接损失、预期收益损失或其他后果性损失承担责任。

9.6 Onward Transfer Controls（后续传输控制）

如子处理者处理活动构成受限跨境传输，GloryScience 将在适用法律要求范围内采取合理措施确保该等子处理者受适用的数据传输机制、合同义务或其他合法保障措施约束。

---

10. International Data Transfers

第十条 跨境数据传输

10.1 Processing Locations（数据处理地点）

默认情况下，客户数据主要存储于阿里云国际云新加坡区域。

为提供服务、灾难恢复、安全防护、技术支持、从节点访问、日志分析、子处理者服务、AI 辅助功能或履行法律义务，相关数据可能在其他司法辖区被访问、处理、缓存、备份或传输。

为避免疑义，跨境数据处理可能包括以下不同场景：

- **Storage Location（存储地）：** 客户数据的主要云托管、主要存储或主要备份地点；默认情况下为阿里云国际云新加坡区域，除非适用的 Order Form、DPA、Security Addendum、服务配置或双方书面约定另有明确规定；
- **Support Access Location（支持访问地）：** GloryScience 或其授权人员为支持、安全、运维、实施、故障排查或服务连续性目的远程访问相关数据的地点；
- **Subprocessor Processing Location（子处理者处理地）：** 子处理者提供云基础设施、支持、监控、通知、日志、支付、安全、AI 辅助功能或其他服务时处理数据的地点；
- **AI Service Invocation Location（AI 服务调用地）：** 在客户启用 AI 辅助功能且适用时，相关输入、输出或上下文数据可能在阿里云国际云新加坡区域、相关 AI 服务提供商或模型相关处理地点、从节点、边缘节点、缓存节点或其他必要地点被调用、传输、缓存或处理。

GloryScience 将根据服务运营需要，采取合理措施管理跨境数据访问与处理风险。具体数据区域、从节点、子处理者及处理地点，以适用的 Order Form、DPA、Security Addendum、服务配置、子处理者清单或双方书面约定为准。

10.2 Transfer Mechanisms（跨境传输机制）

在适用数据保护法律要求的情况下，GloryScience 可支持使用适用的跨境数据传输机制，包括但不限于：

- 欧盟委员会标准合同条款（European Commission Standard Contractual Clauses，“**EU SCCs**”）；
- 英国国际数据传输附录（UK International Data Transfer Addendum to the EU SCCs）或英国国际数据传输协议（UK International Data Transfer Agreement，“**UK IDTA**”）；
- 其他适用法律认可的数据传输机制。

若客户或相关个人数据受 EU GDPR 或 UK GDPR 约束，且 GloryScience 或其子处理者对该等个人数据的处理构成 Restricted Transfer，则双方同意在适用法律要求的范围内适用 EU SCCs、UK Addendum、UK IDTA 或其他适用传输机制。除双方另有书面约定外：

- 客户作为 controller 向 GloryScience 作为 processor 传输个人数据的场景，适用 EU SCCs Module 2（Controller-to-Processor）；
- 客户作为 processor 向 GloryScience 作为 subprocessor 传输个人数据的场景，适用 EU SCCs Module 3（Processor-to-Processor）；
- 对于受 UK GDPR 约束的 Restricted Transfer，适用 UK Addendum 或 UK IDTA 中与相关传输结构相匹配的机制；
- 本 DPA 第 1 条、Annex 1 和 Annex 6 构成 EU SCCs 所需的 Annex I 的相关处理说明；
- 本 DPA Annex 2 构成 EU SCCs 所需的 Annex II 的技术与组织措施说明；
- 本 DPA Annex 3 构成 EU SCCs 所需的 Annex III 的子处理者说明。

如适用法律、客户审查或签约流程要求双方单独签署、补充或更新 EU SCCs、UK Addendum、UK IDTA、转移影响评估文件或其他数据传输文件，双方应在合理范围内配合完成。除 Restricted Transfer 所必需的强制条款外，本 DPA 及《Oneasy SaaS 服务协议》的责任限制、审计限制、费用承担、客户责任和服务边界继续适用。

10.3 Security and Supplementary Measures（安全与补充保护措施）

GloryScience 将根据处理活动性质及合理商业标准，采取适当的技术与组织安全措施，以降低跨境数据传输相关风险。

相关措施可能包括：

- 访问控制与权限管理；
- 数据传输加密；
- 安全监控与日志审计；
- 数据隔离或最小化访问原则；
- 子处理者管理；
- 合理的安全防护及风险缓解措施。

10.4 Customer Responsibility（客户责任）

客户作为相关数据的数据控制者、数据处理指示方或其他责任主体，应负责：

- 确保其向 GloryScience 提供或允许处理相关数据具备合法依据；
- 履行适用法律要求的通知、告知及同意义务；
- 在适用情况下完成跨境数据传输影响评估（TIA / TRA）或其他合规评估；
- 确认其将个人数据、订户数据、电信运维数据、网络安全数据或通信元数据传输至 GloryScience 及其子处理者的合法性；
- 确保其使用本服务符合其所属司法辖区的法律法规要求。

10.5 Compliance Cooperation（合规配合）

在适用法律要求范围内，双方应在合理必要范围内相互配合，以满足适用的数据保护及跨境数据传输合规要求。

但除法律明确要求或双方另有书面约定外，GloryScience 不承诺针对特定国家或地区法律提供定制化法律合规意见、监管合规保证、数据本地化承诺、政府访问承诺、公共部门合规承诺或特定行业合规认证。

---

11. Data Subject Requests

第十一条 数据主体请求

若 GloryScience 收到与客户数据有关的数据主体请求，GloryScience 可将该请求转交客户处理。客户作为数据控制者或适用法律下功能上相当的责任主体负责最终响应数据主体。

在合理范围内，GloryScience 将通过产品功能或技术支持协助客户履行数据主体权利请求，包括访问、更正、删除、限制处理、数据可携或反对处理等请求。

如客户请求 GloryScience 提供超出标准服务功能或标准技术支持范围的协助，GloryScience 可要求客户提供必要信息、验证请求合法性、确认请求范围，并承担合理协助费用，除非适用法律另有强制要求。

---

12. Deletion and Return of Data

第十二条 数据删除与返还

服务终止后，客户可根据 Oneasy 服务提供的可用功能，在三十（30）日内导出、返还或迁移客户数据。客户也可在该期间内书面请求 GloryScience 删除或协助返还特定客户数据，但该等请求应受技术可行性、账户验证、安全要求、数据隔离状态、备份机制及适用法律限制约束。

除客户在导出期内提出明确且可执行的返还或删除请求外，在服务终止后，GloryScience 将在九十（90）日内完成客户数据删除流程。

备份、安全日志、审计日志、系统日志、法定留存数据、账单记录、争议解决所需数据、欺诈防控记录、安全事件记录及 GloryScience 为保护其合法权益或遵守法律义务所需的数据除外；该等数据应按照 Oneasy 的保留政策、适用法律和安全要求进行隔离、限制访问或删除。

除适用法律要求或为安全、合规、审计、争议解决、账单、记录保存、欺诈防控或合法权益保护目的所必要外，GloryScience 将不再主动为商业目的处理已隔离的客户数据。

---

13. Audit and Compliance

第十三条 审计与合规协助

13.1 Documentation Review（文件审查）

客户可合理要求 GloryScience 提供与数据保护和安全措施相关的说明文件、合规摘要、安全控制概要、TOMs 摘要、企业客户安全问卷回复或第三方审计 / 认证报告摘要（如有且可披露）。GloryScience 可对该等材料进行脱敏、摘要化或保密处理，以保护 Oneasy、其客户、子处理者、供应商、系统安全和商业秘密。

13.2 Information Necessary to Demonstrate Compliance（合规证明信息）

在适用数据保护法律要求范围内，GloryScience 将提供其合理掌握且为证明其履行本 DPA 下处理者义务所必要的信息。该等信息提供应受保密义务、信息安全限制、商业秘密保护、第三方保密限制、其他客户数据保护及合理请求范围限制约束。

13.3 Audit Limits（审计限制）

除非双方另有书面约定，Oneasy 和 GloryScience 无义务接受：

- 不受限制的现场审计；
- 影响服务安全或稳定性的渗透测试；
- 要求披露其他客户数据、Oneasy 商业秘密、源代码、底层基础设施细节或高敏感安全信息的审计；
- 过度频繁、不成比例或不合理的审计请求；
- 未遵守合理通知、范围、保密、费用、时间、人员、工具和安全限制的审计。

13.4 Enterprise Audit（企业客户审计）

对于受严格监管的企业客户，双方可另行约定合理的审计范围、频率、保密义务、费用承担和操作方式。

除适用法律强制要求或发生经确认的重大安全事件外，直接审计通常应以每十二（12）个月一次为限，并应优先通过文件审查、安全问卷、第三方报告摘要、会议说明或远程访谈方式完成。任何现场审计、渗透测试、扫描测试或高敏感安全评估均须经 GloryScience 事先书面同意，并遵守 Oneasy 的安全测试规则和服务稳定性要求。

---

14. AI Processing Restrictions

第十四条 AI 数据处理限制

除非客户明确书面授权，GloryScience 不会：

- 使用可识别客户数据训练通用人工智能模型；
- 将客户数据用于与提供服务无关的 AI 商业化目的；
- 向第三方 AI 服务商出售或出租客户数据。

Oneasy 服务中的 AI 输出仅作为辅助性建议。客户不得在未经人工审核与确认的情况下，将 AI 输出直接应用于生产网络环境。

如客户启用 AI 辅助功能，客户应避免向该等功能提交超出必要范围的个人数据、通信内容、敏感个人信息、订户敏感数据或受监管数据。GloryScience 可根据安全、合规、模型供应商限制或技术可行性，对 AI 相关数据输入、输出、保留、调用或功能范围施加合理限制。

---

15. Telecom-Specific Compliance

第十五条 电信行业特殊合规

客户理解并确认，客户数据可能包含网络拓扑、设备配置、运维日志、IP 地址、MAC 地址、性能数据、故障数据、告警数据、订户相关标识或其他电信运维相关信息。

客户应自行确认：

- 是否有权接入、管理和操作相关网络设备；
- 是否有权将相关数据提交至 Oneasy 服务；
- 是否有权授权 GloryScience 及其子处理者通过 Oneasy 服务为提供服务而访问、处理、传输、存储或分析相关数据；
- 是否需要依据本地电信监管法律、通信保密法律、网络安全法律、关键基础设施法律或数据保护法律取得授权、备案、许可、审批或同意；
- 是否涉及最终用户通信数据、订户数据、通信内容或受监管通信元数据。

客户不得通过 Oneasy 服务上传、处理或存储任何非法监听、未授权通信截获、通信内容、违反适用通信保密法律的数据，或未经适当授权的订户、最终用户或第三方数据。

Oneasy 服务提供 SaaS 平台、网络 OAM 辅助、技术支持、诊断、分析、建议、工作流或自动化辅助能力，不构成 GloryScience 作为客户网络运营者、电信运营商、公共通信服务提供者、客户终端用户服务提供者或客户监管义务承担方。

---

16. Liability

第十六条 责任限制

本 DPA 下的责任限制适用《Oneasy SaaS 服务协议》第九条。若适用法律明确禁止限制某类责任，则在该等法律禁止限制的范围内不适用责任限制。

为避免疑义，除适用法律明确禁止限制或双方另有书面约定外，GloryScience 不对因客户违法上传或处理数据、客户未取得必要授权或同意、客户网络或设备环境、客户配置错误、客户未履行本地通信或数据保护合规义务、第三方设备或服务、不可抗力、或客户将 AI 输出未经人工审核直接用于生产网络而导致的损失承担超出主协议责任限制的责任。

---

17. Governing Law and Disputes

第十七条 法律适用与争议解决

本 DPA 适用香港特别行政区法律。

因本 DPA 引起或与本 DPA 有关的任何争议，应按照《Oneasy SaaS 服务协议》第十二条约定的争议解决机制处理。

---

18. Order of Precedence

第十八条 文件优先级

如不同文件之间存在冲突，除双方通过 Order Form、SOW、Enterprise SLA 或其他经授权书面文件明确另有约定外，适用以下优先级：

1. Order Form / Subscription Order / SOW / Enterprise SLA；
2. Data Processing Agreement / DPA；
3. Security Addendum；
4. Oneasy SaaS 服务协议；
5. Oneasy 支付退款条款；
6. Oneasy 隐私政策；
7. Oneasy Cookie 政策；
8. Oneasy 网站使用条款。

但对于纯粹支付、退款、账单、自动续费、拒付、逾期付款事项，以支付退款条款为准；对于公开网站访问事项，以网站使用条款为准；对于 Cookie 和追踪技术事项，以 Cookie 政策为准；对于个人数据处理事项，以 DPA 为准；对于安全控制事项，以 Security Addendum 为准，但如安全事项同时涉及个人数据处理、跨境传输、个人数据泄露通知或数据保护法律义务，则 DPA 优先。

Annex 1 — Processing Description

附件一：数据处理说明

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

Item	Description
	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)

附件二：技术与组织安全措施

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

附件三：子处理者类别

GloryScience may use subprocessors in the following categories:

Category	Purpose
Cloud Infrastructure Provider	Hosting, storage, compute, networking, backup, disaster recovery

Category	Purpose
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

附件四：电信运维数据提示

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

附件五：GDPR Article 28 对照表

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

附件六：跨境传输与数据流说明

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

Data Flow / Processing Scenario	Typical Location / Role	Purpose	Safeguards / Notes
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.

注：“新加坡区域”指 Oneasy 服务的主要云托管、主要数据处理与主要存储区域。香港是 GloryScience International Limited 的注册和合同管辖主体所在地，不应被解释为 Oneasy 服务默认主存储区域，除非适用的 Order Form、DPA、Security Addendum、服务配置、子处理者清单或双方书面约定另有明确规定。

注：“支付处理服务商”主要适用于 GloryScience 作为独立控制者处理账单/支付数据的场景；仅在其代表客户处理 DPA 范围内个人数据时才构成子处理者。