

POLÍTICA DE PRIVACIDAD DE LOS SERVICIOS SAAS DE ONEASY

Última actualización: 25 de junio de 2026

Fecha de entrada en vigor: 25 de junio de 2026

GloryScience International Limited, sociedad constituida conforme a las leyes de la Región Administrativa Especial de Hong Kong ("GloryScience", "nosotros" o la "Empresa"), es la operadora de Oneasy SaaS Platform ("Oneasy" o el "Servicio").

Reconocemos la importancia de sus Datos Personales y nos comprometemos a brindarles una protección razonable, adecuada y acorde con la naturaleza del Servicio. Esta Política de Privacidad de los Servicios SaaS (la "Política") explica de manera clara y transparente cómo GloryScience trata sus Datos Personales cuando usted utiliza el sitio web o la plataforma SaaS de Oneasy o interactúa con nosotros.

Esta Política forma parte del Contrato de Servicios SaaS de Oneasy (el "Contrato Principal"). En caso de conflicto relativo al tratamiento de Datos Personales, prevalecerán el Anexo de Tratamiento de Datos aplicable ("DPA") celebrado o incorporado por referencia y las normas imperativas de la Legislación Aplicable. Los controles específicos de seguridad, acceso remoto, respuesta a incidentes, conservación de registros y medidas técnicas y organizativas se regirán por el Security Addendum, el DPA u otro documento de seguridad acordado. Sus derechos y obligaciones serán determinados en última instancia por la legislación de protección de datos competente y por los suplementos regionales que publiquemos. Lea esta Política antes de utilizar el Servicio. Si no está de acuerdo, no lo utilice.

1. ALCANCE Y DEFINICIÓN DE ROLES

1.1 Alcance

Esta Política se aplica al sitio web de Oneasy, incluido www.oneasy.cc y sus subdominios, a la plataforma SaaS de Oneasy y a las API, los canales de soporte y las comunicaciones comerciales relacionados. No se aplica a sitios, aplicaciones o servicios operados por terceros, aunque sean accesibles mediante el Servicio.

1.2 Roles Esenciales

De acuerdo con las principales leyes mundiales de protección de datos, podremos desempeñar distintos roles en diferentes actividades de tratamiento.

(A) GloryScience como Responsable del Tratamiento

Podremos actuar como Responsable del Tratamiento de los Datos Personales necesarios para prestar, operar, proteger y mejorar el Servicio. Esto normalmente comprende datos de cuenta, facturación y transacciones; registros de uso y diagnóstico; registros de seguridad y cumplimiento; e información recopilada mediante cookies y tecnologías similares para la operación del sitio, análisis, seguridad y optimización.

(B) GloryScience como Encargado del Tratamiento

Respecto de los datos que usted, como nuestro Tenant, cargue, genere o administre durante el uso de Oneasy ("Datos del Tenant"), GloryScience normalmente actúa como Encargado del Tratamiento. Estos datos pueden incluir información de equipos, configuraciones de red, indicadores de rendimiento y registros de operación y mantenimiento. En este rol, tratamos los Datos del Tenant únicamente conforme al Contrato Principal, el DPA y sus configuraciones e instrucciones dentro del Servicio. Las obligaciones específicas de GloryScience como Encargado respecto de los Datos Personales contenidos en los Datos del Tenant se establecerán en el DPA aplicable.

(C) Tenant como Responsable del Tratamiento

El Tenant es el Responsable o sujeto equivalente respecto de sus Datos del Tenant y es responsable de manera independiente de cumplir las leyes de privacidad, protección de datos, confidencialidad de las comunicaciones, telecomunicaciones, ciberseguridad y demás normas aplicables a sus actividades, incluida la existencia de una base jurídica válida.

1.3 Interpretación en Jurisdicciones que no Utilizan los Términos del GDPR

Cuando la ley no utilice los términos "Controller" y "Processor", o les atribuya un significado diferente, las referencias al Responsable, Encargado, Tenant y proveedor de servicios se interpretarán conforme a los roles y obligaciones funcionalmente más cercanos previstos en dicha ley, sin ampliar las obligaciones legales de GloryScience más allá de lo establecido por ella.

2. INFORMACIÓN QUE RECOPIAMOS

Observamos el principio de minimización y solo recopilamos información necesaria para fines específicos, explícitos y legítimos.

2.1 Datos de Cuenta y Configuración

Para crear y administrar su cuenta, recopilamos nombre, correo electrónico, contraseña y, cuando usted los proporcione, cargo, departamento, empresa, rol de cuenta, permisos y datos similares.

2.2 Datos de Suscripción y Pago

Para gestionar suscripciones y pagos, recopilamos razón social, dirección de facturación, identificación fiscal, historial de pedidos, plan, estado del pago y datos de facturación. Los datos completos de tarjetas son tratados directamente por proveedores de pago seleccionados y alineados con las normas del sector; nosotros no almacenamos los datos completos de la tarjeta.

2.3 Datos de Uso, Operación y Mantenimiento

Para operar el Servicio, diagnosticar fallas y mejorar el rendimiento, recopilamos automáticamente dirección IP, identificador del dispositivo, tipo de navegador, fecha y hora de acceso, registros de uso, indicadores de rendimiento, informes de errores, inicios de sesión, llamadas API, incidentes de seguridad y otros Datos Operativos de la Plataforma necesarios.

2.4 Datos del Tenant

Son Datos del Tenant todos los datos empresariales ingresados, cargados, configurados, autorizados para lectura, permitidos para generación o generados por el Servicio a partir de equipos, redes o configuraciones del Usuario. El Tenant controla su contenido; como Encargado, no somos responsables de dicho contenido. El Tenant deberá determinar si los datos cargados, integrados, transmitidos, tratados o autorizados para tratamiento están sujetos a normas de telecomunicaciones, confidencialidad de las comunicaciones, ciberseguridad o protección de datos.

Los Datos del Tenant pueden incluir configuraciones de equipos de ISP, direcciones IP y MAC, identificadores, información de OLT u ONU, topología, registros operativos, fallas, alarmas, indicadores, telemetría, registros de acceso remoto, resultados de SNMP walk, salidas de CLI o API, copias de seguridad de configuraciones, capturas de paquetes, diagnósticos y análisis. En algunas jurisdicciones, podrán constituir Datos Personales, datos de telecomunicaciones regulados, metadatos de comunicaciones, datos de ciberseguridad, información comercial sensible o datos de infraestructura crítica. El Tenant evaluará su naturaleza y asumirá el cumplimiento correspondiente.

La aceptación del Contrato Principal, creación del Tenant, incorporación de equipos, configuración de credenciales, habilitación de Agent, VPN, Connector, API, SNMP, TR-069, TR-369, CLI, Syslog, ACS o NMS, carga de MIB, OID, resultados de SNMP walk, salidas de CLI o API, copias de seguridad, registros, capturas, scripts, plantillas, materiales de equipos, fabricantes o terceros, o autorización a Oneasy para leer, generar o tratar dichos materiales constituye una instrucción y autorización del cliente a GloryScience para tratar los Datos del Tenant pertinentes a efectos de protección de datos.

Para evitar dudas, esta Política trata principalmente los Datos Personales y la parte de los Datos del Tenant que los contenga. En cuanto a MIB, OID, SNMP walk, CLI, API, OMCI, firmware, materiales de fabricantes, documentos internos, plantillas, scripts, capturas, muestras de registros u otros Materiales Técnicos de Terceros que no sean Datos Personales, el origen de los derechos, autorización de uso, confidencialidad, propiedad intelectual, secretos comerciales y responsabilidad se regirán por el Contrato Principal, el Security Addendum, el Order Form, el SOW o los términos específicos.

2.5 Registros de Comunicaciones

Cuando usted se comunica con soporte, participa en una consulta comercial o capacitación, abre un ticket o envía comentarios, conservamos las comunicaciones, los adjuntos y la información de diagnóstico proporcionada voluntariamente.

2.6 Datos Personales Sensibles

Si el caso de uso inevitablemente implica Datos Personales sensibles, categorías especiales, contenido de comunicaciones u otros datos altamente sensibles, obtenga previamente el consentimiento expreso y por escrito de GloryScience y confirme que dispone de todas las bases jurídicas, avisos, consentimientos, autorizaciones, registros o aprobaciones necesarios. GloryScience podrá rechazar el tratamiento por motivos de seguridad, cumplimiento, viabilidad técnica o riesgo comercial.

2.7 Cookies y Tecnologías Similares

Podremos utilizar cookies, identificadores de registros y tecnologías similares para la operación del sitio, mantenimiento de sesión, seguridad, preferencias necesarias, pagos, prevención del fraude y cumplimiento. Conforme a la Política de Cookies vigente en la fecha de su última actualización, Oneasy no utiliza cookies no esenciales de análisis, publicidad, marketing, remarketing, seguimiento entre sitios, conversiones o chat e interacción con clientes. Consulte la Política de Cookies para conocer categorías, fines, conservación y controles.

2.8 Verificación Humana Cloudflare Turnstile

Para prevenir abuso automatizado, registros maliciosos, accesos anómalos y otros riesgos, el sitio podrá utilizar Cloudflare Turnstile. Al acceder a una página que lo utilice, el navegador podrá comunicarse con los servidores de Cloudflare para verificar si la solicitud proviene de una persona real. Según sea necesario para su operación, Cloudflare podrá tratar dirección IP, datos del navegador y dispositivo, entorno de acceso e información para análisis de riesgos. El servicio se utiliza exclusivamente para seguridad, reducción de ataques automatizados y estabilidad, no para publicidad ni seguimiento entre sitios.

Consulte la Cloudflare Turnstile Privacy Policy: <https://www.cloudflare.com/turnstile-privacy-policy/>

3. CÓMO UTILIZAMOS LA INFORMACIÓN Y BASES JURÍDICAS

Solo tratamos Datos Personales cuando existe una base jurídica válida.

3.1 Ejecución de un Contrato

El tratamiento de datos de cuenta y pago y la prestación de las funciones esenciales son necesarios para ejecutar el Contrato Principal.

3.2 Intereses Legítimos

Con base en nuestros intereses legítimos, podremos monitorear la seguridad, prevenir fraude y abuso, mejorar y desarrollar productos, mantener la estabilidad, atender solicitudes de soporte y realizar la administración interna necesaria. Cuando sea obligatorio, evaluaremos los impactos en la privacidad y adoptaremos medidas razonables para reducir riesgos innecesarios. En la medida exigida y razonablemente posible, podremos proporcionar información sobre estas actividades.

3.3 Cumplimiento de una Obligación Legal

Podremos tratar y conservar información según sea necesario para cumplir obligaciones fiscales, contables, regulatorias, de aplicación de la ley, seguridad, solución de controversias y demás obligaciones legales.

3.4 Consentimiento

Cuando sea obligatorio, obtendremos consentimiento para tratamientos no necesarios para operar el Servicio, como determinadas comunicaciones de marketing. Usted podrá retirarlo en cualquier momento conforme a la Legislación Aplicable.

4. TRATAMIENTO DE LOS DATOS DEL TENANT

4.1 Principios

Tratamos los Datos del Tenant únicamente conforme al Contrato Principal, DPA, Security Addendum, Order Form, SOW, funciones del producto y configuraciones, cargas, autorizaciones de lectura, permisos de generación u otras instrucciones registradas. Incorporar equipos, configurar credenciales, habilitar Agent, VPN, Connector, API, SNMP, TR-069, TR-369, CLI, Syslog, ACS o NMS, cargar archivos, autorizar lectura de salidas o permitir la generación de SNMP walk, salidas CLI o API, copias de seguridad, capturas, registros o diagnósticos podrá constituir una instrucción dentro del Servicio.

Podremos rechazar una instrucción manifiestamente contraria a la ley. Si consideramos que una instrucción podría infringirla, notificaremos al Tenant y explicaremos las razones cuando sea razonablemente posible, dándole la oportunidad de presentar una base jurídica o alternativa. Las partes buscarán de buena fe una solución compatible con la ley, el contrato y la seguridad. Si no hay acuerdo y creemos razonablemente que ejecutarla generará responsabilidad legal, riesgo de seguridad o incumplimiento de una obligación frente a terceros, podremos suspenderla sin incurrir en incumplimiento.

4.2 Responsabilidades del Tenant

El Tenant declara y garantiza que posee el derecho y la base jurídica para tratar todos los Datos del Tenant; que ha proporcionado los avisos exigidos a Titulares, suscriptores, usuarios finales, empleados y demás personas pertinentes; que ha obtenido los consentimientos, autorizaciones, licencias, registros, aprobaciones internas u otras bases necesarias; y que ha implementado una gestión de permisos, segmentación de red y controles adecuados.

Para equipos, redes, interfaces, cuentas, credenciales, MIB, OID, SNMP walk, salidas CLI o API, OMCI, firmware, configuraciones, registros, capturas, scripts, plantillas u otros materiales integrados o tratados por Oneasy, el Tenant deberá confirmar y obtener los derechos de propiedad, operación, administración, mantenimiento autorizado, divulgación, reproducción, uso y sublicencia; exenciones de confidencialidad; licencias de fabricantes; autorizaciones contractuales y regulatorias; y avisos o consentimientos de usuarios finales. Podremos confiar razonablemente en las configuraciones, cargas, autorizaciones y registros del Servicio sin verificar la cadena de autorización en cada tratamiento.

4.3 Asistencia

Si un Titular ejerce directamente ante nosotros un derecho relativo a Datos del Tenant, normalmente lo orientaremos a contactar al Tenant como Responsable o sujeto responsable. Dentro de límites razonables, asistiremos al Tenant mediante funcionalidades, API, exportación o soporte técnico para cumplir sus obligaciones.

5. TRANSFERENCIAS INTERNACIONALES DE DATOS

El Servicio es global y sus Datos Personales podrán ser accedidos, tratados o transferidos fuera de su país o región.

5.1 Salvaguardas

Cuando una transferencia internacional requiera salvaguardas, utilizaremos mecanismos reconocidos, como las Cláusulas Contractuales Tipo de la Unión Europea (SCC), mecanismos del Reino Unido u otros aplicables, junto con medidas técnicas y organizativas razonables, como control de acceso, cifrado, registros y monitoreo de seguridad.

5.2 Transferencia Internacional de los Datos del Tenant

Por defecto, la región principal de almacenamiento de los Datos del Tenant es la región de Singapur de Alibaba Cloud International. Para prestar el Servicio, mejorar el rendimiento, recuperar desastres, proteger la seguridad, brindar soporte, utilizar subencargados y funciones asistidas por IA, permitir acceso mediante nodos regionales o cumplir obligaciones legales, los datos podrán ser accedidos, tratados, almacenados en caché, respaldados o transferidos en otras jurisdicciones.

Podremos utilizar Alibaba Cloud International y otros proveedores evaluados de nube, redes, CDN, seguridad, registros, monitoreo, pagos, atención al cliente e IA como proveedores o subencargados. La lista de

subencargados relevantes, categorías de servicio, fines y principales lugares de tratamiento será publicada o proporcionada mediante el sitio, la consola, la documentación u otro medio razonable.

Las regiones, los nodos secundarios, de contingencia, borde, registros, caché o copias de seguridad, lugares de soporte, subencargados y llamadas de IA serán los definidos en el Contrato Principal, DPA, Security Addendum, Order Form, configuración, lista de subencargados o acuerdo escrito. Salvo acuerdo expreso, indicar la región principal no constituye un compromiso de localización ni garantiza que todos los accesos, tratamientos, cachés, copias, registros, soportes o servicios ocurran en una sola jurisdicción.

El cliente será responsable, como Responsable o equivalente, de las evaluaciones de impacto y adecuación, avisos, consentimientos, registros y otros procedimientos de transferencia. Esto no impide el tratamiento internacional necesario, por GloryScience como Responsable, de datos de cuenta, registros, pagos, soporte, cumplimiento y operación para los fines del Artículo 3.

6. INTERCAMBIO Y DIVULGACIÓN DE INFORMACIÓN

No vendemos sus Datos Personales. Solo compartimos información en las siguientes situaciones:

6.1 Proveedores de Servicios y Subencargados

Podremos compartir la información necesaria con socios de alojamiento, redes, CDN, pagos, análisis, comunicaciones, seguridad, registros, monitoreo, atención al cliente, IA y otros servicios necesarios, incluidos Alibaba Cloud International y demás proveedores evaluados. Adoptaremos medidas comercialmente razonables para exigir obligaciones de confidencialidad, protección y seguridad acordes con el servicio. Respecto de subencargados relevantes de Datos del Tenant, las notificaciones, objeciones y modificaciones se registrarán por el DPA, el Contrato Principal u otro documento aplicable.

La lista vigente de subencargados relevantes, categorías, fines y ubicaciones será publicada o proporcionada por canales razonables. Al incorporar o sustituir un subencargado que pueda afectar sustancialmente el tratamiento de Datos del Tenant, GloryScience notificará al cliente y proporcionará un mecanismo razonable de objeción conforme al DPA o los documentos aplicables.

6.2 Requisitos Legales

Podremos divulgar información para responder a un proceso legal válido, exigencia regulatoria, solicitud de autoridad u orden judicial; proteger la seguridad personal; defender los derechos o bienes de GloryScience, clientes o terceros; o cuando la ley lo exija.

6.3 Reorganización Empresarial

Podremos divulgar información en la medida necesaria en una fusión, adquisición, financiación, venta de activos, transferencia, reorganización u operación similar, adoptando medidas razonables para mantener una protección y confidencialidad adecuadas.

7. SEGURIDAD Y CONSERVACIÓN DE DATOS

7.1 Normas de Seguridad

Implementaremos y mantendremos medidas técnicas y organizativas comercialmente razonables contra el acceso, divulgación, alteración, pérdida o destrucción no autorizados de Datos Personales y Datos del Tenant. Podrán incluir control de acceso, autenticación, cifrado en tránsito, protección en reposo cuando corresponda, registros, monitoreo, gestión de vulnerabilidades, confidencialidad del personal y respuesta a incidentes.

Los controles específicos, seguridad de acceso remoto, Agent y VPN, conservación, vulnerabilidades, auditoría y medidas técnicas y organizativas se registrarán por el Security Addendum, DPA, Contrato Principal o documento acordado.

7.2 Notificación de Incidentes de Seguridad

Si confirmamos un incidente que pueda afectar de manera importante sus Datos Personales, Datos del Tenant o la seguridad del Servicio, notificaremos al cliente conforme a la ley y sin demora indebida. Cuando sea razonablemente posible y exista información preliminar confirmada, normalmente enviaremos una notificación inicial dentro de las setenta y dos (72) horas posteriores a la confirmación.

En la medida de la información disponible, la notificación indicará la naturaleza, las categorías o sistemas afectados, los impactos conocidos o probables, los controles, medidas de mitigación y corrección adoptados o en curso, las acciones recomendadas al cliente y el canal de seguimiento. Podremos complementar la información a medida que avancen la investigación, el análisis forense y la respuesta.

7.3 Copias de Seguridad y Recuperación

Adoptaremos una estrategia razonable de copias de seguridad conforme a las necesidades empresariales y las prácticas del sector. La frecuencia, conservación, recuperación, objetivo de tiempo de recuperación (RTO) y objetivo de punto de recuperación (RPO), cuando constituyan compromisos vinculantes, se definirán en un SLA, Order Form, Security Addendum o acuerdo específico. Salvo acuerdo expreso, RTO y RPO no constituyen niveles de servicio vinculantes.

7.4 Responsabilidades de Seguridad del Usuario

Internet, la nube y el acceso remoto no son absolutamente seguros. El Usuario deberá administrar cuentas, permisos, identidades de administradores, API Keys, tokens, credenciales de VPN, Agent y equipos, segmentación y aprobaciones internas. Salvo exigencia legal o acuerdo expreso, no respondemos por filtraciones, interrupciones o pérdidas causadas por falta de protección de credenciales, actuación indebida de Usuarios Autorizados, configuración incorrecta de permisos, segmentación insuficiente, vulnerabilidades en equipos o sistemas del cliente, falta de actualización de Agent o VPN o uso de una red inadecuada. Recomendamos MFA en cuentas administrativas, revisión periódica de usuarios y permisos y rotación de API Keys, tokens y credenciales privilegiadas.

7.5 Conservación

Conservamos Datos Personales y Datos del Tenant solo durante el período necesario para los fines de esta Política, el Contrato Principal, DPA, Security Addendum o la ley. Los plazos específicos y las reglas de eliminación, anonimización, exportación y conservación excepcional de cuentas, Datos del Tenant, registros operativos y de seguridad, copias de seguridad, finanzas y controversias se definirán en los documentos aplicables, la configuración o la ley.

8. DERECHOS DE LOS TITULARES DE LOS DATOS

Conforme a la ley aplicable, usted podrá tener derechos de acceso, rectificación, supresión, limitación, portabilidad, retiro del consentimiento y oposición a determinados tratamientos.

Cómo ejercer sus derechos: si es Usuario Autorizado de un Tenant, contacte primero al administrador de su organización. Si es Responsable directo de la cuenta o el administrador no puede atenderlo, escriba a support@oneasy.cc. Podremos verificar su identidad por seguridad.

Respecto de solicitudes de Usuarios Autorizados o relativas a Datos del Tenant, el Tenant, como Responsable o sujeto responsable, deberá responder oportunamente conforme a la ley. GloryScience brindará asistencia razonable mediante funcionalidades, API, exportación o soporte.

Respecto de Datos Personales tratados por GloryScience como Responsable, responderemos a solicitudes verificables dentro de los plazos legales. En la medida permitida, podremos rechazar o limitar solicitudes manifiestamente infundadas, excesivamente repetitivas, que afecten derechos de terceros, involucren secretos comerciales o riesgos de seguridad o cuya divulgación esté prohibida.

9. EXENCIONES Y LIMITACIÓN DE RESPONSABILIDAD

9.1 Servicio Proporcionado "Tal Cual"

En la máxima medida permitida, el Servicio y sus contenidos se proporcionan "tal cual" y "según disponibilidad". Salvo compromiso expreso en el Contrato Principal, DPA, Security Addendum o acuerdo escrito, no ofrecemos garantías expresas o implícitas, incluidas comerciabilidad, idoneidad para un fin particular, no infracción, operación ininterrumpida o ausencia de errores. Esta limitación no se aplica a dolo o culpa grave de GloryScience ni a responsabilidad que la ley prohíba limitar.

9.2 Situaciones Específicas

Salvo exigencia legal o acuerdo expreso, no respondemos por interrupción, retraso, pérdida, daño o indisponibilidad causada directa o indirectamente por: (1) fuerza mayor fuera de nuestro control, incluidos desastre, guerra, disturbio, ciberataque a gran escala, interrupción de backbone, falla importante de nube pública o restricción regulatoria; (2) actos del Usuario o Usuario Autorizado, falla de equipo, conexión, permisos, filtración de credenciales, aprobación insuficiente o incumplimiento de recomendaciones; (3) inobservancia de guías, documentación, seguridad o procesos razonables; (4) mantenimiento programado o de emergencia para actualización, corrección o riesgo; o (5) falla de terceros, red o equipo del cliente, firmware, interfaz privada, nube o proveedor de telecomunicaciones.

9.3 Asignación de Responsabilidad

La asignación de responsabilidad por tratamiento, incidentes o limitaciones relacionados con el Servicio se regirá por el Contrato Principal, DPA, Security Addendum y la Legislación Aplicable.

10. LEY APLICABLE, CONTROVERSIAS Y COMPROMISO DE CUMPLIMIENTO

10.1 Ley Aplicable

Esta Política, su interpretación, validez y ejecución y las controversias derivadas de ella se regirán por las leyes de la Región Administrativa Especial de Hong Kong, con exclusión de sus normas sobre conflicto de leyes.

10.2 Cumplimiento de Leyes de Protección de Datos

En la medida en que tengan jurisdicción y resulten aplicables, GloryScience cumplirá los requisitos imperativos de protección de datos, incluidos, cuando corresponda, el EU GDPR, UK GDPR, PDPO de Hong Kong, PDPA de Singapur y otras leyes aplicables. Esto no significa la aceptación incondicional de leyes de jurisdicciones sin conexión efectiva con el tratamiento.

Los conflictos sobre ley y controversias seguirán sujetos a la Cláusula 10.1 y al Contrato Principal, sin impedir que los Titulares presenten una reclamación ante la autoridad competente o ejerzan derechos irrenunciables.

10.3 Solución de Controversias

Las controversias relacionadas con esta Política se resolverán conforme al Contrato Principal, incluida la posibilidad de arbitraje ante el Hong Kong International Arbitration Centre (HKIAC) cuando dicho mecanismo sea aplicable. El arbitraje no perjudica el derecho del Titular a presentar una reclamación ante la autoridad competente.

10.4 Actualizaciones

Podremos revisar esta Política. Las modificaciones sustancialmente desfavorables, incluida una ampliación importante de la recopilación, un nuevo intercambio relevante, una reducción significativa de la protección o un impacto adverso en los derechos, se notificarán al administrador del Tenant con treinta (30) días de antelación mediante correo electrónico, consola, sitio web u otro medio razonable.

Si la ley exige un plazo distinto, o si la seguridad, la ley, la regulación, la continuidad o un riesgo urgente requieren una vigencia más rápida, actuaremos conforme a la ley y a prácticas comerciales razonables. El uso posterior a la entrada en vigor implica aceptación; si no está de acuerdo, el Usuario deberá dejar de utilizar el Servicio y podrá gestionar la terminación o exportación conforme al Contrato Principal.

11. CONTÁCTENOS

Si tiene preguntas sobre esta Política o nuestras prácticas de privacidad, contacte a nuestro equipo de protección de datos:

Asuntos jurídicos y de protección de datos: legal@oneasy.cc

Soporte técnico general: support@oneasy.cc

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