# CONTRATO DE ENCARGO DEL TRATAMIENTO DE DATOS PERSONALES LEMONTECH

**Producto: Lemonflow**

Lemontech SpA, rol único tributario N° 99.511.620-0, representada por don Ezequiel Rabinovich, cédula de identidad N° 24.881.069-6, ambos domiciliados en Avenida Apoquindo 4501, oficinas 1901 y 1903, comuna de Las Condes, Santiago, Chile, en adelante indistintamente "LEMONTECH" o el "Encargado"; y "EL CLIENTE", persona natural o jurídica que contrata los servicios de Lemontech desde cualquier país, territorio o jurisdicción y que acepta los términos de este Contrato, en adelante el "Responsable".

Las partes suscriben el presente Contrato de Encargo de Tratamiento de Datos Personales (en adelante, el "Contrato" o el "DPA"), que forma parte del Acuerdo Marco de Servicios suscrito entre ellas, con el objeto de regular el tratamiento de datos personales que el Encargado realiza por cuenta del Responsable en el servicio LEMONFLOW, y manifiestan lo siguiente:

I.- Que EL CLIENTE es responsable de los tratamientos de los datos personales que ingresa, o hace ingresar por sus usuarios, a la plataforma.

II.- Que, para la ejecución del servicio prestado, LEMONTECH, en su calidad de Encargado, tendrá acceso o tratará datos personales por cuenta del Responsable. Los tratamientos que se realizarán, dependiendo de los módulos contratados, son los siguientes:

- **Creación y administración de cuentas de usuario:** registro, habilitación y gestión de cuentas de acceso a la plataforma, incluyendo la configuración de credenciales, asignación de roles (Administrador, Editor, Solicitante), permisos diferenciados por módulo, estructuración de áreas organizacionales y equipos de trabajo. Cuando el Responsable utilice un proveedor de identidad externo (SSO), la plataforma gestionará la autenticación delegada mediante los atributos transmitidos por dicho proveedor.
- **Gestión de solicitudes operativas y de derechos:** recepción, seguimiento y resolución de solicitudes internas de servicios legales (revisión de contratos y solicitudes financieras) y de solicitudes de ejercicio de derechos de protección de datos (acceso, rectificación, supresión, oposición, portabilidad y bloqueo) formuladas por los titulares ante el Responsable.
- **Gestión de riesgos corporativos y compliance normativo:** identificación, evaluación, tratamiento y monitoreo de riesgos con responsables asignados; seguimiento del estado de implementación de normativas legales aplicables (entre ellas la Ley Nº 21.719) y sus requisitos de cumplimiento, con objetivos trazados por persona responsable. Algunos de estos módulos cuentan con funcionalidades asistidas por inteligencia artificial (IA) que vinculan los registros de la plataforma con flujos gestionados por un proveedor externo

de IA; dicho tratamiento queda sujeto a lo establecido en el número 9 de la cláusula IV y en el Anexo III.

- **Canal de denuncias (Ley N° 21.643, "Ley Karin", y Ley N° 20.393):** recepción, registro, asignación e investigación de denuncias por acoso laboral u otras irregularidades, incluyendo datos del denunciante, del investigador designado y de las personas involucradas.
- **Repositorio documental:** almacenamiento, organización y trazabilidad de metadatos de documentos legales y corporativos (contratos, NDAs, licitaciones, anexos), con registro del creador, fecha y entidad o proyecto asociado.
- **Auditoría interna e integridad del sistema:** registro automático e inmutable de toda acción realizada por usuarios en la plataforma (creación, modificación, eliminación, visualización), con identificación del usuario ejecutor, dirección IP del acceso, objeto afectado y descripción detallada del cambio campo a campo.
- **Generación de reportes de compliance:** elaboración de reportes y dashboards sobre el estado de solicitudes, riesgos, tareas e incidentes, incluyendo métricas individualizadas por responsable asignado.
- **Gestión de contratos (módulo opcional):** elaboración, negociación, aprobación y firma electrónica de contratos, con la participación de contrapartes, abogados externos, aprobadores y firmantes invitados por el Responsable.

III.- Que, con el fin de proteger dichos datos personales y dar cumplimiento a la Normativa de Protección de Datos, celebran el presente Contrato con sujeción a las siguientes cláusulas.

## I. Objeto y definiciones

El presente Contrato regula el tratamiento de datos personales que realizará LEMONTECH, en calidad de Encargado, por cuenta de EL CLIENTE, en su calidad de Responsable. Dicho tratamiento se efectuará conforme al Acuerdo Marco de Servicios (MSA), a la propuesta comercial o contrato de prestación de servicios aplicable, y a la Normativa de Protección de Datos.

Para efectos de este Contrato: (a) "Normativa de Protección de Datos" significa la Ley N° 19.628, sobre protección de datos personales, en su texto modificado por la Ley N° 21.719, y su normativa complementaria, así como toda otra ley de protección de datos personales que resulte aplicable al tratamiento en razón del lugar de establecimiento del Responsable o de residencia de los titulares, conforme a la cláusula XIII y al Anexo IV; (b) "Instrucciones documentadas" significa las instrucciones del Responsable contenidas en el MSA, en este Contrato y sus anexos, en la configuración de la plataforma que realicen el Responsable o sus usuarios, y en las demás instrucciones que el Responsable comunique por escrito; (c) "Subencargado" significa todo tercero que trate datos personales del Responsable por cuenta

del Encargado; y (d) "Incidente de seguridad" significa toda vulneración de las medidas de seguridad que ocasione la destrucción, pérdida, alteración, comunicación o acceso no autorizados, accidentales o ilícitos, de datos personales tratados en virtud de este Contrato.

Quedan excluidos de este encargo los tratamientos que LEMONTECH realiza con fines propios, en calidad de responsable, tales como la gestión de la relación comercial y de facturación con EL CLIENTE, la recepción y gestión de solicitudes de soporte (datos de contacto del usuario y descripción del requerimiento), la analítica de uso de la plataforma, las comunicaciones comerciales y la seguridad de la plataforma, los que se rigen por su aviso de privacidad. El acceso que el personal de soporte requiera a los datos alojados en la plataforma para resolver una solicitud se rige por este Contrato.

En lo relativo al tratamiento de datos personales, lo dispuesto en este Contrato prevalecerá sobre el MSA y sobre cualquier otro documento suscrito entre las partes. Si resultan aplicables cláusulas contractuales tipo conforme a la cláusula X o al Anexo IV, éstas prevalecerán sobre este Contrato en caso de contradicción.

## II. Duración

Este Contrato tendrá la misma vigencia que el MSA y que la prestación de los servicios contratados, incluidas sus prórrogas. Las obligaciones de confidencialidad, devolución y supresión de los datos, y las demás que por su naturaleza deban subsistir, se mantendrán vigentes tras su término.

A la finalización del servicio, el Encargado, según instrucción del Responsable, suprimirá o devolverá todos los datos personales tratados y sus copias, salvo que una norma legal exija su conservación. Los plazos y condiciones de la devolución y supresión, incluidas las copias de seguridad, se rigen por la cláusula IX.

## III. Identificación de la información afectada

Para la ejecución de las acciones derivadas del cumplimiento del objeto de este encargo, EL CLIENTE, responsable del tratamiento, pone a disposición del Encargado la información que se describe a continuación:

- **Datos identificativos:** nombre, apellidos, correo electrónico corporativo, identificadores fiscales (RUT de personas naturales y jurídicas, RUC, RFC). En el caso de terceros externos (contrapartes contractuales), nombre completo y cargo del representante legal firmante.
- **Datos de contacto:** número de teléfono (campo opcional para usuarios internos), correo electrónico del creador de documentos.
- **Datos profesionales y organizacionales:** cargo, área funcional, rol en plataforma, equipos asignados, responsabilidades en tareas, riesgos y normativas.

- **Datos de acceso y autorización:** credenciales de autenticación (contraseña almacenada en formato hasheado, no legible), roles y permisos diferenciados por módulo, estado de verificación de cuenta, fecha de creación. Cuando el Responsable configure un proveedor de identidad externo (SSO), se tratarán además los atributos transmitidos por dicho proveedor (tipo, nombre del proveedor, mapeo de atributos y alcances de autorización).
- **Datos de actividad laboral y comportamiento digital:** logs de auditoría con timestamp exacto, dirección IP del acceso, tipo de acción ejecutada, objeto afectado con su ID, descripción campo a campo de cada cambio, incluyendo contenido de comunicaciones internas y menciones entre usuarios. Se registra adicionalmente la fecha y hora en que cada usuario recibió y visualizó las notificaciones del sistema.
- **Datos contractuales y financieros:** nombre de empresa contraparte, condiciones contractuales, montos de instrumentos financieros (boletas de garantía, contratos), vigencia, glosa de servicios, número de licitación.
- **Datos del canal de denuncias, sujetos a confidencialidad reforzada:** identidad del denunciante, descripción de los hechos denunciados, identidad del investigador designado y de las personas involucradas o investigadas. Pueden incluir datos sensibles.
- **Datos del módulo de gestión de contratos (cuando sea contratado):** nombre y correo electrónico de los participantes externos; y, para la firma electrónica, nombre, correo electrónico y documento de identidad del firmante y, si el Responsable las configura, verificaciones adicionales de identidad (código por SMS, validación biométrica, verificación contra el Registro Civil o certificado electrónico), que se resuelven en la infraestructura del proveedor de firma.

Las categorías de titulares y la descripción del tratamiento constan en el Anexo I.

El Responsable determina qué datos ingresa a la plataforma. El Encargado no es responsable del contenido de los documentos, comentarios o registros que el Responsable o sus usuarios carguen, sin perjuicio de su obligación de tratarlos conforme a este Contrato.

## IV. Obligaciones de LEMONTECH

El Encargado se obliga, y hará que su personal y sus Subencargados se obliguen, a:

1. Tratar los datos personales únicamente para la ejecución de este encargo y conforme a las Instrucciones documentadas del Responsable, incluso en lo relativo a transferencias internacionales. El Encargado no tratará los datos para fines propios, salvo lo previsto en el número 9 de esta cláusula, ni los comunicará o utilizará con otra finalidad.
2. Informar inmediatamente al Responsable si, a su juicio, una instrucción infringe la Normativa de Protección de Datos, pudiendo suspender su ejecución mientras el Responsable la confirma o modifica.

3. Guardar secreto y confidencialidad respecto de los datos personales a los que acceda en virtud de este encargo, incluso después de su término, y asegurar que las personas autorizadas para tratarlos se hayan comprometido por escrito a respetar dicha confidencialidad o estén sujetas a una obligación legal de confidencialidad.

4. Asistir al Responsable, mediante medidas técnicas y organizativas apropiadas, en la atención de las solicitudes de los titulares para el ejercicio de sus derechos de acceso, rectificación, supresión, oposición, portabilidad y bloqueo, y del derecho a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos, así como de los demás derechos que reconozca la Normativa de Protección de Datos aplicable. Si el Encargado recibe directamente una solicitud, la trasladará al Responsable sin dilación indebida y, en todo caso, dentro de los dos (2) días hábiles siguientes a su recepción, sin responderla por sí mismo salvo instrucción del Responsable.

5. Aplicar las medidas técnicas y organizativas de seguridad descritas en el Anexo II, apropiadas al riesgo del tratamiento, que comprenden la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento, la de restaurar oportunamente la disponibilidad y el acceso a los datos ante un incidente físico o técnico, y un proceso de verificación periódica de su eficacia. El Encargado podrá actualizar dichas medidas siempre que no disminuya el nivel de protección.

6. No comunicar los datos a terceros, salvo a los Subencargados conforme a la cláusula VI, a otros encargados que el Responsable indique por escrito, o cuando lo exija una ley o una resolución de autoridad competente. En este último caso, el Encargado informará al Responsable antes de efectuar la comunicación, salvo que la ley lo prohíba, y la limitará a lo estrictamente requerido.

7. No adoptar por cuenta propia decisiones basadas únicamente en el tratamiento automatizado de los datos ni elaborar perfiles de los titulares. Las funcionalidades de la plataforma que generan reportes, métricas o sugerencias se ejecutan por instrucción del Responsable, a quien corresponde decidir su uso respecto de los titulares.

8. Asistir al Responsable, considerando la naturaleza del tratamiento y la información de que disponga, en la elaboración de evaluaciones de impacto en protección de datos cuando sean exigibles conforme al artículo 15 ter de la Ley N° 19.628 o a la normativa aplicable, y en las consultas previas a la autoridad de control que correspondan.

9. **Respecto de las funcionalidades basadas en inteligencia artificial:** (i) utilizar los proveedores de inteligencia artificial indicados en el Anexo III únicamente a través de sus servicios empresariales, bajo términos contractuales que les prohíben utilizar los datos del Responsable para entrenar sus modelos; (ii) no utilizar los datos del Responsable para entrenar modelos de inteligencia artificial de terceros; y (iii) por instrucción del Responsable, que éste otorga mediante la aceptación de este Contrato,

utilizar información derivada del uso del servicio para mejorar las funcionalidades del servicio, exclusivamente en forma agregada, en un entorno cerrado y controlado, sin comunicarla a terceros, sin que los resultados permitan identificar al Responsable ni a los titulares, y excluyendo credenciales, conforme a los Términos y Condiciones del servicio.

10. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratarlos.
11. Cooperar con la Agencia de Protección de Datos Personales y con las demás autoridades de control competentes, a solicitud del Responsable o cuando la ley lo exija.

El Encargado podrá comunicar los datos a otros encargados del tratamiento del mismo Responsable, de acuerdo con sus instrucciones. En este caso, el Responsable identificará, de forma previa y por escrito, la entidad a la que deben comunicarse los datos, los datos a comunicar y las medidas de seguridad que se aplicarán a la comunicación.

## V. Obligaciones de EL CLIENTE

El Responsable se obliga a:

1. Contar con una base de licitud para cada tratamiento que encomiende al Encargado y acreditarla cuando sea requerido, conforme a la Normativa de Protección de Datos.
2. Asegurar que los datos personales se recojan de fuentes lícitas, con fines específicos, explícitos y lícitos, y que su tratamiento se limite al cumplimiento de dichos fines.
3. Informar a los titulares, en los términos que exija la Normativa de Protección de Datos, sobre el tratamiento de sus datos, incluida la intervención de encargados y la transferencia internacional de los datos a los países indicados en la cláusula X.
4. Determinar si carga en la plataforma datos sensibles, datos de niños, niñas y adolescentes u otras categorías especialmente protegidas, cumplir respecto de ellos los requisitos especiales que establezca la Normativa de Protección de Datos e informar al Encargado si su tratamiento requiere medidas adicionales a las del Anexo II.
5. Si el Responsable no tiene domicilio en Chile, registrar y mantener actualizado un correo electrónico u otro medio de notificación válido para que los titulares y la Agencia de Protección de Datos Personales puedan contactarlo.
6. Cumplir los demás deberes, principios y obligaciones que le impone la Normativa de Protección de Datos aplicable, incluida, cuando corresponda, la realización de evaluaciones de impacto.
7. Velar, de forma previa y durante todo el tratamiento, por el cumplimiento de la normativa en materia de protección de datos por parte del Encargado.
8. **Respecto del canal de denuncias:** configurar los accesos de modo que solo las personas designadas para la investigación conozcan la identidad del denunciante y los

antecedentes de la denuncia, y cumplir la normativa aplicable a dichos procedimientos, incluidas, en Chile, la Ley N° 21.643 y la Ley N° 20.393.

9. Designar un correo electrónico para las comunicaciones derivadas de este Contrato y mantenerlo actualizado.

**VI. Subcontratación**

El Responsable autoriza de manera general al Encargado para subcontratar el tratamiento de datos personales con terceros proveedores ("Subencargados") cuando ello sea necesario para la prestación del servicio, conforme a las condiciones de esta cláusula.

**Servicios auxiliares.** Se exceptúan del régimen de aviso previsto en el párrafo siguiente los proveedores de soporte general (por ejemplo, herramientas internas de mensajería o productividad) cuyo acceso a datos personales del Responsable sea meramente incidental y no constituya el objeto del tratamiento encomendado. Los proveedores de alojamiento o infraestructura que almacenen o procesen dichos datos no quedan comprendidos en esta excepción. Los proveedores auxiliares estarán sujetos a obligaciones de confidencialidad y seguridad equivalentes a las de este Contrato.

**Integraciones.** Las integraciones con servicios de terceros que el Responsable o sus usuarios activen (por ejemplo, Google Calendar o Microsoft Outlook) no constituyen subencargo. El tratamiento en dichos servicios se rige por los términos que el Responsable o el usuario hayan aceptado con su proveedor.

**Lista y aviso de cambios.** Los Subencargados vigentes se indican en el Anexo III. El Encargado mantendrá dicha lista actualizada y disponible para el Responsable, e informará toda incorporación o sustitución de un Subencargado con al menos quince (15) días corridos de antelación a su entrada en vigor, mediante la actualización de la lista publicada y aviso al correo de contacto designado por el Responsable.

**Derecho de oposición.** Dentro de ese plazo, el Responsable podrá oponerse fundadamente al cambio, únicamente por razones concretas de riesgo para la protección de los datos personales (por ejemplo, insuficiencia de garantías de seguridad o incumplimiento normativo del Subencargado). El Encargado evaluará la objeción de buena fe. Si no es posible ofrecer una alternativa razonable, el Responsable podrá poner término anticipado al servicio específico afectado, sin penalidad, sin que ello le dé derecho a exigir la mantención de un Subencargado distinto para su caso particular.

**Responsabilidad.** El Encargado celebrará con cada Subencargado un contrato escrito que le imponga obligaciones de protección de datos equivalentes a las de este Contrato, y garantizará que trate los datos solo para las finalidades autorizadas, siga las instrucciones del Responsable y aplique medidas de seguridad equivalentes a las exigidas al Encargado. El incumplimiento de un Subencargado no exime al Encargado de su responsabilidad ante el Responsable.

**Transferencias internacionales.** Las transferencias internacionales de datos personales derivadas del uso de Subencargados se rigen por la cláusula X.

## VII. Notificación de incidentes de seguridad

El Encargado notificará al Responsable, sin dilación indebida y en un plazo máximo de setenta y dos (72) horas desde que tome conocimiento, todo Incidente de seguridad que afecte datos personales tratados en virtud de este Contrato. La notificación se efectuará al correo electrónico designado por el Responsable e incluirá la información relevante para documentar el incidente y, en su caso, comunicarlo a la autoridad de control y a los titulares.

Si se dispone de ella, se facilitará, como mínimo, la siguiente información:

1. Descripción de la naturaleza del incidente, incluidas, cuando sea posible, las categorías y el número aproximado de titulares afectados, y las categorías y el número aproximado de registros de datos personales afectados.
2. El nombre y los datos de contacto del Delegado de Protección de Datos o de otro punto de contacto en el que pueda obtenerse más información.
3. Descripción de las posibles consecuencias del incidente.
4. Descripción de las medidas adoptadas o propuestas para remediar el incidente, incluidas, si procede, las medidas adoptadas para mitigar sus posibles efectos negativos.

Si no es posible facilitar toda la información simultáneamente, se facilitará de manera gradual y sin dilación indebida.

El Encargado adoptará sin demora las medidas necesarias para contener el incidente y mitigar sus efectos; colaborará con el Responsable en el reporte a la Agencia de Protección de Datos Personales conforme al artículo 14 sexies de la Ley N° 19.628, o a la autoridad que corresponda según el Anexo IV, y en la comunicación a los titulares; y mantendrá un registro de los incidentes. Salvo que una obligación legal propia lo exija, el Encargado no comunicará el incidente a autoridades ni a titulares sin la previa autorización del Responsable.

## VIII. Responsabilidad de las partes

Cada parte responderá, en la medida en que le corresponda, de las sanciones administrativas y de los daños y perjuicios causados por el incumplimiento de las obligaciones que la Normativa de Protección de Datos le impone.

Cada parte mantendrá indemne a la otra de las pérdidas, reclamaciones, multas y gastos razonables, incluidos honorarios de abogados, que ésta sufra como consecuencia directa del incumplimiento de este Contrato o de la Normativa de Protección de Datos por la parte infractora, en la medida permitida por la ley. Esta obligación estará sujeta a las limitaciones de responsabilidad establecidas en el MSA, salvo en caso de dolo o culpa grave.

Si el Encargado trata los datos con una finalidad distinta, los comunica o los utiliza en incumplimiento de este Contrato, será considerado responsable del tratamiento respecto de dicho tratamiento y responderá personalmente de las infracciones en que incurra.

**IX. Conservación, devolución y supresión de los datos**

El Encargado conservará los datos personales del Responsable conforme a las siguientes reglas:

a) **Datos de la plataforma:** se conservan mientras esté vigente el servicio. El Responsable puede modificarlos o eliminarlos desde la plataforma en cualquier momento, salvo los registros de auditoría, que son inmutables y se conservan durante toda la vigencia del servicio.

b) **Término del servicio:** durante la vigencia del servicio y a su término, el Responsable podrá extraer sus datos en un formato estructurado y de uso común. Terminado el servicio, el Encargado mantendrá un respaldo de la información por un plazo de doce (12) meses, salvo que el Responsable ordene su supresión en un plazo menor, y luego la suprimirá. Lo anterior se entiende sin perjuicio de los datos cuya conservación exija una disposición legal o reglamentaria, los que el Encargado conservará solo durante el plazo legalmente exigible y para esa finalidad.

c) **Copias de seguridad:** el Encargado mantiene recuperación a un punto en el tiempo (PITR) de las últimas 24 horas y copias de seguridad diarias con una retención de un (1) año, cifradas y almacenadas de forma redundante en AWS (Estados Unidos), por lo que los datos suprimidos de los entornos productivos pueden permanecer en las copias de seguridad hasta por un (1) año. Dichas copias solo se utilizarán para restaurar el servicio ante incidentes.

d) A solicitud del Responsable, el Encargado certificará por escrito la supresión efectuada.

**X. Ubicación del tratamiento y transferencias internacionales**

**Ubicación del tratamiento.** Los datos del Responsable se alojan en Amazon Web Services, en la región us-east-1 (Norte de Virginia, Estados Unidos) como región principal y us-west-2 (Oregón, Estados Unidos) como región de recuperación ante desastres. El tráfico hacia la plataforma es filtrado por Cloudflare, Inc. a través de su red global. Las funcionalidades de análisis normativo asistido por inteligencia artificial utilizan modelos de OpenAI, con procesamiento en Estados Unidos. Cuando el Responsable contrate el módulo de gestión de contratos, la firma electrónica se realiza a través de los proveedores de firma indicados en el Anexo III.

**Garantías.** Las transferencias internacionales de datos personales a los Subencargados se sustentan en sus respectivos acuerdos de tratamiento de datos, que incorporan cláusulas

contractuales tipo u otras garantías adecuadas, conforme a los artículos 27 y 28 de la Ley N° 19.628.

**Responsables sujetos al RGPD.** Cuando el Responsable esté establecido en el Espacio Económico Europeo o el tratamiento esté sujeto al Reglamento (UE) 2016/679, las partes incorporan por referencia a este Contrato las cláusulas contractuales tipo aprobadas por la Decisión de Ejecución (UE) 2021/914 de la Comisión, Módulo Dos (de responsable a encargado), en las que el Responsable actúa como exportador y el Encargado como importador, con las siguientes opciones: (i) no se incluye la cláusula 7; (ii) cláusula 9, opción 2 (autorización general por escrito), con el plazo de aviso previsto en la cláusula VI; (iii) no se incluye la opción de la cláusula 11 letra a); (iv) cláusula 13: la autoridad de control del Estado miembro en que esté establecido el Responsable; y (v) cláusulas 17 y 18: la legislación y los tribunales del Estado miembro en que esté establecido el Responsable. Los Anexos I, II y III de dichas cláusulas se entienden completados con los Anexos I, II y III de este Contrato. En caso de contradicción, prevalecerán las cláusulas contractuales tipo. Si el tratamiento está sujeto al RGPD del Reino Unido, se aplicará además el International Data Transfer Addendum emitido por la Information Commissioner's Office.

**Otras jurisdicciones.** Cuando el Responsable esté establecido en otra de las jurisdicciones indicadas en el Anexo IV, se aplicarán además las reglas previstas en dicho anexo.

El Encargado informará al Responsable cualquier cambio relevante en la ubicación del tratamiento o en las garantías aplicables, conforme al procedimiento de aviso de la cláusula VI.

## XI. Auditoría

El Encargado pondrá a disposición del Responsable la información necesaria para demostrar el cumplimiento de este Contrato, incluidos sus certificados de seguridad y privacidad vigentes, dentro de los diez (10) días hábiles siguientes a su solicitud. Si dicha información no fuere suficiente, el Responsable, directamente o a través de un auditor independiente sujeto a confidencialidad, podrá realizar una auditoría con aviso previo de al menos quince (15) días hábiles, una vez al año, salvo incidente de seguridad o requerimiento de autoridad competente. La auditoría se realizará en horario hábil, sin afectar la operación del Encargado, y será de cargo del Responsable, salvo que se detecte un incumplimiento grave, en cuyo caso será de cargo del Encargado.

## XII. Delegado de Protección de Datos

El Encargado ha designado como Delegado de Protección de Datos a Makarena Alarcón González, contactable en dpo@lemontech.com, quien actuará como punto de contacto para el Responsable en todas las materias relativas a este Contrato. El Encargado informará sin dilación cualquier cambio en esta designación.

**XIII. Normativa aplicable y jurisdicción**

Este Contrato se rige por las leyes de la República de Chile, sin perjuicio de la aplicación de las normas imperativas de protección de datos personales del país en que esté establecido el Responsable o en que residan los titulares, cuando resulten aplicables al tratamiento. Si dichas normas establecen en una materia un estándar de protección más exigente que este Contrato, las partes aplicarán ese estándar respecto de los datos y titulares sujetos a ellas, conforme al Anexo IV.

Las controversias derivadas de este Contrato se resolverán conforme al mecanismo de solución de controversias pactado en el MSA, salvo lo que dispongan imperativamente las cláusulas contractuales tipo aplicables.

## ANEXO I — DESCRIPCIÓN DEL TRATAMIENTO

**Partes:** Exportador / Responsable: EL CLIENTE, según se identifica en el Acuerdo Marco o propuesta comercial.

**Importador / Encargado:** Lemontech SpA, Avenida Apoquindo 4501, oficinas 1901 y 1903, Las Condes, Santiago, Chile; contacto: dpo@lemontech.com.

**Categorías de titulares:** usuarios de la plataforma (trabajadores y colaboradores del Responsable); contrapartes contractuales y sus representantes; participantes externos en el módulo de gestión de contratos (contrapartes, abogados externos, aprobadores y firmantes); titulares que ejercen derechos de protección de datos ante el Responsable; y denunciantes, personas denunciadas, testigos e investigadores en el canal de denuncias.

**Categorías de datos:** las indicadas en la cláusula III. **Datos sensibles:** no se solicitan; pueden tratarse en el canal de denuncias, en documentos cargados por el Responsable o, si éste la configura, en la validación biométrica de firmantes, que realiza el proveedor de firma. Se aplican las medidas del Anexo II.

**Frecuencia:** continua, durante la vigencia del servicio. **Naturaleza y finalidad:** las descritas en el punto II de la comparecencia y en la cláusula I. **Conservación:** según la cláusula IX. **Transferencias:** según la cláusula X. **Subencargados:** según el Anexo III.

## ANEXO II — MEDIDAS TÉCNICAS Y ORGANIZATIVAS

a) **Cifrado en tránsito:** TLS 1.2 en todas las comunicaciones entre los usuarios y la plataforma y entre sus servicios internos.

b) **Cifrado en reposo:** AES-256 en la base de datos (Amazon RDS PostgreSQL) y en los archivos (Amazon S3), con claves gestionadas mediante AWS Key Management Service y rotación anual.

c) **Alojamiento y segregación:** infraestructura en AWS, con región principal us-east-1 y región de recuperación ante desastres us-west-2, cada una distribuida en tres zonas de disponibilidad; modelo multi-tenant con un schema de base de datos independiente para cada cliente; y archivos, sesiones, tokens y claves de caché segmentados por cliente.

d) **Control de acceso y autenticación:** control de acceso basado en roles (RBAC) configurable por el Responsable; contraseñas gestionadas por Amazon Cognito, sin acceso del Encargado, con política mínima de complejidad; SSO mediante SAML; segundo factor de autenticación (TOTP) que el Responsable puede exigir a todos sus usuarios; bloqueo de la cuenta tras diez intentos fallidos en 15 minutos y limitación de intentos por dirección IP; sesiones gestionadas en el servidor, con cookies httpOnly y Secure y duración máxima y cierre por inactividad configurables por el Responsable; y acceso del personal del Encargado según el principio de mínimo privilegio, con autenticación multifactor obligatoria en los repositorios de código.

e) **Registro de auditoría:** registro permanente e inmutable de la creación, modificación, eliminación, restauración y descarga de datos, con el usuario, la fecha, la dirección IP y los valores anteriores y posteriores, consultable y exportable por el Responsable.

f) **Disponibilidad y recuperación:** arquitectura multi-región activa-pasiva; recuperación a un punto en el tiempo (PITR) de las últimas 24 horas; copias de seguridad según la letra c) de la cláusula IX, con verificación periódica de integridad y restauración; y plan de recuperación ante desastres probado anualmente, con RTO de 4 horas y RPO de aproximadamente 5 minutos, o de 24 horas ante la caída de la región principal.

g) **Desarrollo y operación seguros:** despliegue automatizado y trazable mediante integración y entrega continua (CI/CD); análisis de código estático y dinámico; escaneos de vulnerabilidades con plan de remediación y retest; pruebas de penetración anuales ejecutadas por una empresa externa independiente; Web Application Firewall (Cloudflare); y monitoreo continuo, detección de amenazas y registro centralizado de eventos (SIEM) con alertas en tiempo real.

h) **Gestión de incidentes:** proceso formal alineado con ISO/IEC 27001 e ISO/IEC 27701, con detección continua y alertas en tiempo real, y notificación conforme a la cláusula VII.

i) **Módulo de gestión de contratos:** los participantes externos acceden mediante enlaces de un solo propósito con vigencia de 24 horas, limitados a un contrato y a un rol, reciben solo los datos necesarios para su actuación y pierden el acceso automáticamente al completarla o al cambiar el estado del contrato; las descargas se realizan mediante direcciones firmadas con vigencia de una hora; y la firma electrónica se realiza a través de proveedores acreditados.

j) **Canal de denuncias:** acceso a las denuncias según los roles y permisos que configure el Responsable; seguimiento por el denunciante mediante una sesión temporal de 15 minutos, sin credenciales persistentes.

k) **Inteligencia artificial:** los datos se envían a los proveedores de modelos de lenguaje a través de su API empresarial, en tiempo real y aislados por sesión, y dichos proveedores tienen prohibido contractualmente utilizarlos para entrenar sus modelos.

l) **Personal:** obligaciones de confidencialidad y capacitación periódica en seguridad de la información, protección de datos y gobernanza de IA.

m) **Certificación:** el Encargado mantiene un Sistema de Gestión de Seguridad de la Información certificado bajo ISO/IEC 27001 y un Sistema de Gestión de Privacidad de la Información certificado bajo ISO/IEC 27701.

n) **Revisión:** el Encargado revisará estas medidas al menos una vez al año o ante cambios significativos, sin disminuir el nivel de protección aquí descrito.

**ANEXO III — SUBENCARGADOS**

Lista vigente al 12 de noviembre de 2026. Las modificaciones se informarán conforme a la cláusula VI.

| **Nombre** | **¿Cuál es su función?** | **¿Dónde se encuentra?** | **Base jurídica** |
|---|---|---|---|
| Amazon Web Services, Inc. | Alojamiento de infraestructura, bases de datos, autenticación (Amazon Cognito), envío de correos transaccionales (Amazon SES) y copias de seguridad | EE.UU.: us-east-1 (Norte de Virginia), principal; us-west-2 (Oregón), recuperación ante desastres | DPA de AWS con cláusulas contractuales tipo |
| Cloudflare, Inc. | Web Application Firewall y filtrado de tráfico | Red global | DPA de Cloudflare con cláusulas contractuales tipo |
| PostHog, Inc. | Analítica de uso del producto | EE.UU. | DPA de PostHog con cláusulas contractuales tipo de la UE (Módulo Dos) y adhesión al |

| Nombre | ¿Cuál es su función? | ¿Dónde se encuentra? | Base jurídica |
|---|---|---|---|
| | | | EU-U.S. Data Privacy Framework |
| OpenAI, L.L.C. | Modelos de lenguaje para el análisis normativo asistido por IA, vía API empresarial | EE.UU. | DPA de OpenAI con cláusulas contractuales tipo; los datos enviados por API no se utilizan para entrenar modelos |
| Firma Segura, S. de R.L. de C.V. (Mifiel) | Firma electrónica en el módulo de gestión de contratos (mercado mexicano) | México | Acuerdo de tratamiento de datos (DPA) suscrito con Lemontech |
| Agile Ingeniería y Consultoría S.A. (Agile) | Firma electrónica en el módulo de gestión de contratos (mercado chileno) | Chile | Acuerdo de tratamiento de datos (DPA) suscrito con Lemontech |

**ANEXO IV — REGLAS POR JURISDICCIÓN**

Este anexo se aplica según el país en que esté establecido el Responsable o, cuando la normativa local así lo disponga, según el país de residencia de los titulares. En lo no previsto en él rige el cuerpo de este Contrato.

a) **Chile:** Ley N° 19.628, sobre protección de datos personales, en su texto modificado por la Ley N° 21.719. Este Contrato da cumplimiento al artículo 15 bis de dicha ley.

b) **Espacio Económico Europeo y Reino Unido:** se aplican las cláusulas contractuales tipo y el addendum indicados en la cláusula X.

c) **Colombia:** este Contrato constituye el contrato de transmisión de datos personales previsto en el artículo 25 del Decreto 1377 de 2013, compilado en el Decreto Único Reglamentario 1074 de 2015. El Encargado tratará los datos conforme a la política de tratamiento de la información del Responsable y a los principios de la Ley 1581 de 2012.

d) **Perú:** el Encargado actúa como encargado del tratamiento conforme a la Ley N° 29733, Ley de Protección de Datos Personales, y su Reglamento aprobado por Decreto

Supremo N° 016-2024-JUS. Corresponde al Responsable cumplir las obligaciones de registro o comunicación ante la Autoridad Nacional de Protección de Datos Personales que le resulten aplicables, incluidas las relativas a flujos transfronterizos.

e) **México:** la entrega de datos al Encargado constituye una remisión conforme a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares publicada en el Diario Oficial de la Federación el 20 de marzo de 2025. El Encargado tratará los datos conforme al aviso de privacidad del Responsable y a sus instrucciones.

f) **Argentina:** el tratamiento se rige además por el artículo 25 de la Ley N° 25.326. Las transferencias a países que no cuenten con un nivel adecuado de protección se sustentarán en las cláusulas contractuales modelo aprobadas por la Agencia de Acceso a la Información Pública.

g) **Brasil:** cuando el tratamiento esté sujeto a la Lei Geral de Proteção de Dados Pessoais (Lei N° 13.709/2018), las transferencias internacionales se sustentarán en las cláusulas contractuales estándar aprobadas por la Resolución CD/ANPD N° 19/2024, que las partes incorporan por referencia.

h) **Otras jurisdicciones:** el Encargado colaborará con el Responsable para incorporar, mediante adenda, las garantías adicionales que exija la normativa aplicable.